В ПОИСКАХ КИБЕРДОВЕРИЯ

Международный союз электросвязи

В ПОИСКАХ КИБЕРДОВЕРИЯ

Д-р Хамадун И. Туре

Генеральный секретарь

Международного союза электросвязи

и

Постоянная группа по мониторингу

информационной безопасности

Всемирной федерации ученых

НОЯБРЬ 2014 ГОДА

Официальное уведомление

Авторы лично обладают интеллектуальными правами на свои работы. Источники третьих сторон цитируются в соответствии с правилами. Международный союз электросвязи (МСЭ) не несет ответственности за содержание внешних источников, включая внешние веб-сайты, на которые ссылаются в данной публикации.

Ни МСЭ, ни любой другой человек, выступающий от его лица, не несет ответственности за последствия использования информации, содержащейся в данной публикации.

Правовая оговорка

Главы в данной публикации отражают мнение отдельных авторов, которые не поддерживаются или не призваны отражать мнение любой организации, в которой они могут работать или быть связаны. Упоминание и отсылки на определенные страны, компании, продукты, инициативы или руководящие указания никоим образом не означают, что они поддерживаются или рекомендованы МСЭ, авторами, или любыми другие организациями, с которыми связаны авторы, по сравнению с другими, имеющими такую же природу, которые не упоминаются.

Выражение признательности

Генеральный Секретарь МСЭ и Всемирная федерация ученых хотели бы поблагодарить Хеннинга Вегенера и всех авторов, которые позволили собрать вместе их мнения по этой новой всемирной проблеме. Генеральный Секретарь выражает признательность проф. Антонино Дзикики, президенту WFS, и свою искреннюю благодарность Марко Обизо, который руководил изданием данной публикации и координировал его, а также группе МСЭ по кибербезопасности, в частности Алексу Гамеро Гарридо, Алие Абдул Разак, Деспойне Сарейдаки, Энтони Драммонду, Притаму Малуру и Рошин Авотар-Маури и многим другим в МСЭ и WFS, без участия которых эта публикация была бы невозможна.

Если у вас есть какие-либо замечания, пожалуйста, свяжитесь с группой по кибербезопасности Международного союза электросвязи по адресу: cybersecurity@itu.int.

Содержание

Стр.

О Международном союзе электросвязи

Международный союз электросвязи (МСЭ) – ведущее учреждение Организации Объединенных Наций по вопросам информационно-коммуникационных технологий и глобальный координатор для правительств и частного сектора в области развития сетей и услуг.

Важнейшая роль МСЭ после Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) и Полномочной конференции МСЭ 2006 года заключается в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ). Главы государств и правительств, другие глобальные лидеры, участвующие в ВВУИО, а также Государства – Члены МСЭ поручили МСЭ предпринять конкретные шаги к сдерживанию угроз и опасностей, связанных с информационным обществом. Для выполнения этого поручения Генеральный секретарь МСЭ д-р Хамадун И. Туре объявил в 2007 году о начале Глобальной программы кибербезопасности (ГПК) как основы международного сотрудничества в области кибербезопасности с участием многих заинтересованных сторон, направленного на достижение синергии с существующими и будущими инициативами и партнерами. Основное внимание в ГПК уделяется следующим пяти направлениям работы: меры правового характера, меры технического и процедурного характера, организационные структуры, создание потенциала и международное сотрудничество.

К числу важнейших инициатив по оказанию помощи Государствам-Членам в создании потенциала в сфере кибербезопасности под эгидой ГПК и при поддержке глобальных партнеров относятся:

- программа в области национальной группы CIRT (Группа реагирования на компьютерные инциденты), в соответствии с которой осуществляется оценка национальной группы CIRT, практическое применение национальной группы CIRT и тренировочные занятия по кибербезопасности на основании запросов от Государств-Членов;
- создание региональных центров кибербезопасности, призванных стать катализаторами расширения регионального сотрудничества, координации и совместной деятельности для решения проблемы растущих киберугроз;
- проект "Повышение кибербезопасности в наименее развитых странах", в рамках которого МСЭ оказывает помощь НРС в расширении их возможностей, потенциала, готовности, навыков и знаний в области кибербезопасности;
- Глобальный индекс кибербезопасности (GCI) – показатель уровня развития кибербезопасности каждого государства, который направлен на обеспечение правильной мотивации стран к наращиванию своих усилий в области кибербезопасности. Конечная цель заключается в содействии формированию глобальной культуры кибербезопасности и превращению ее в один из основных элементов информационно-коммуникационных технологий.

О Всемирной федерации ученых

Всемирная федерация ученых (WFS) была основана в Эриче, Сицилия в 1973 году группой известных ученых, возглавляемой Исидором Исааком Раби и Антонино Дзикики. С тех пор к Федерации присоединилось много других ученых, в том числе Чжэндао Ли, Лаура Ферми, Юджин Вигнер, Поль Дирак и Петр Капица.

Федерация WFS это свободное объединение, которое включает в себя более 10 000 ученых из 110 стран. Все ее члены разделяют одни цели и идеалы и вносят добровольный вклад с целью поддержания принципов Федерации. Федерация способствует международному сотрудничеству в области науки и технологии среди ученых и исследователей всех частей мира – с севера, юга, востока и запада. Федерация и ее члены стремятся к идеалам свободного обмена информацией, в котором научные открытия и достижения более не ограничены малым кругом избранных. Цель состоит в обмене знаниями между людьми всех национальностей, с тем чтобы каждый мог пользоваться достижениями научного прогресса.

Создание Всемирной федерации ученых стало возможным благодаря существованию в Эриче центра научной культуры, названного в честь физика Этторе Майорана, ***Фонда и центра научной культуры Этторе Майорана*** (Центра). Этот Центр, который получил название "Университета третьего тысячелетия", стал мировым центром образования. С момента своего создания в 1963 году Центр провел 123 школьные программы и 1497 курсов для 103 484 участников (125 из которых являются Нобелевскими лауреатами), приехавших из 932 университетов и лабораторий 140 стран.

Центр Этторе Майорана явился предшественником Всемирной федерации ученых и ее действий по смягчению чрезвычайных ситуаций глобального масштаба. Всемирная федерация ученых незамедлительно определила 15 **чрезвычайных ситуаций глобального масштаба** и приступила к организации противодействия этим угрозам. Одним из ее главных достижений стала выработка Полем Дираком, Петром Капицей и Антонино Дзикики в 1982 году Заявления Эриче, ясно определяющего идеалы Федерации и выдвигающего ряд предложений по претворению этих идеалов в жизнь. Другой важной вехой стало проведение серии Международных семинаров по проблемам ядерной войны, которые оказали огромное влияние на снижение опасности ядерной катастрофы для всей планеты и, в конечном счете, способствовали окончанию Холодной войны. В 1986 году в результате действий группы видных ученых (большая часть которых были членами WFS) была основана **Всемирная лаборатория** Международного Центра научной культуры. Всемирная лаборатория ICSC была создана в Женеве с целью достижения целей, указанных в Заявлении Эриче.

В 2001 году Федерация WFS создала свою Постоянную группу по мониторингу (PMP) информационной безопасности. Ее отчет "*В целях всемирного порядка киберпространства: устранение угроз от киберпреступности до кибервойны*"

являлся одним из руководящих документов, созданных гражданским обществом в Организации Объединенных Наций в ходе Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), которая впервые была проведена в Женеве в 2003 году. Группа PMP опубликовала множество статей по кибербезопасности и кибервойнам, а также регулярно представляет вопросы информационной безопасности как важнейшую тему безопасности в масштабах планеты на пленарных заседаниях WFS, проводимых ежегодно в августе в Эриче. В августе 2009 года группа PMP была так обеспокоена возможностью того, что кибервойны разрушат общество и приведут к ненужному ущербу и страданиям, что она подготовила проект **Декларации Эриче о принципах киберстабильности и кибермира**, которая была принята Пленумом WFS по случаю 42-го собрания Международных семинаров по чрезвычайным ситуациям планетарного масштаба в Эриче 20 августа 2009 года. Декларация была разослана всем Государствам – Членам Организации Объединенных Наций.

Декларация была разослана всем Государствам – Членам Организации Объединенных Наций, и с ней, а также со всеми остальными декларациями, публикациями и внутренними документами Постоянной группы по мониторингу информационной безопасности можно ознакомиться на веб-сайте Группы по адресу: www.unibw.de/infosecur.

Председателем PMP является посол Хеннинг Вегенер. Следующие члены группы внесли свой вклад в данную публикацию:

Члены группы, внесшие вклад в данную публикацию

Мона Аль-Ашкар

Д-р Мона Аль-Ашкар Джаббур имеет степень доктора философии в области частного права. Являлась заведующей кафедрами права и научных исследований Ливанского университета с 1998 по 2009 год, а также консультантом и куратором в области реализации базы данных по правовым вопросам в Министерстве юстиции Кувейта.

В настоящее время является профессором права факультета права Ливанского университета, профессором – научным сотрудником Ливанского центра правовой информатики, основателем и президентом Ливанской ассоциации информационных технологий (LITA), основателем Ливанского центра по вопросам киберпреступности, членом и основателем Панарабской обсерватории по кибербезопасности, а также членом Ассоциации онлайновых арабских писателей, Арабской федерации онлайнового арбитража, юридического комитета по защите ребенка в онлайновой среде при Министерстве социальных дел Ливана, группы франкоговорящих стран при ICANN и ФУИ, Ливанского центра по вопросам интернета (LINC), и Постоянной группы по мониторингу информационной безопасности Всемирной федерации ученых.

Д-р Аль-Ашкар опубликовала множество книг и статей по различным правовым вопросам, некоторые из которых касаются правовой информатики и киберправа, а также отмывания денег и терроризма.

Вильям Барлетта

Вильям Барлетта является адъюнкт-профессором физики Масачуссетского технологического института (MIT) и Лос-анджелесского университета Калифорнии (UCLA). Также является приглашенным профессором факультета экономики университета Любляны, директором институтов США и Кореи по ускорителям частиц и координирующим главным редактором секции А рубрики "Ядерные приборы и методы". Старший советник президента центра по исследованию синхротронного излучения в Триесте, Италия, сопредседатель Постоянной группы по мониторингу (PMP) в области энергетики Всемирной Федерации ученых и член PMP информационной безопасности. Недавно избран председателем Группы по связям с общественностью Американского физического общества (APS). Являлся председателем Форума APS по международной физике и Отдела лучевой физики APS, а также активным членом Комитета APS по международным научным делам.

Редактор четырех книг по теории ускорителей и соавтор четырех книг, касающихся кибербезопасности, конфиденциальности и международного киберправа. Владеет четырьмя патентами и является автором более 170 научных статей. Имеет степень доктора философии в области физики Чикагского университета.

Паван Дуггал

Паван Дуггал признан одним из четырех ведущих мировых адвокатов по киберправу. Оказал существенное международное влияние в качестве эксперта и специалиста в области киберправа и электронного торгового права.

На счету Павана, являющегося практикующим адвокатом верховного суда Индии, новаторская работа по праву в области конвергенции и подвижной связи. В силу этого он выступает в качестве консультанта ЮНКТАД и ЮНЕСКО по киберправу и киберпреступности, соответственно. Кроме того, является членом рабочей группы по правовым вопросам АФАКТ СЕФАКТ ООН, консультантом-экспертом по киберпреступности Совета Европы и членом комитета экспертов по электронной коммерции при Европейской комиссии. Его работа в качестве специалиста-эксперта над учебником по киберправу для Целевой группы "Электронная АСЕАН", а также обозревателя для Азиатского банка развития дополнительно свидетельствует о его всемирном признании в качестве крупного специалиста в этих вопросах. Кроме того, является президентом консалтинговых компаний Cyberlaw Asia и Cyberlaws.Net.

Паван выступал более чем на 1200 конференциях, семинарах и практикумах и написал 42 книги по различным аспектам вышеуказанного законодательства за последние годы.

Более подробная информация о Паване Дуггале представлена по адресу: http://www.linkedin.com/in/pavanduggal.

Соланж Гернаути

Солнаж Гернаути, доктор в области компьютерных наук (Парижский университет), является профессором Лозаннского университета и директором Швейцарской консультативно-исследовательской группы по кибербезопасности. Международно признанный эксперт по вопросам, связанным с кибербезопасностью, киберзащитой, киберпреступностью и управлению рисками ИКТ. Участвовала в нескольких инициативах, организованных международными организациями, государственными и частными учреждениями, исследовательскими центрами и правоохранительными органами, а также другими инстанциями в разных странах. Последние несколько лет уделяет основное внимание разработке комплексного межотраслевого подхода к кибербезопасности в интересах граждан, организаций и государств, будучи новатором в этой области.

Является активным независимым консультантом по вопросам безопасности и влиятельным аналитиком, а также регулярным обозревателем в СМИ. Швейцарская пресса признала ее одной из выдающихся женщин профессиональных и академических кругов. Кавалер ордена Почетного легиона и член Швейцарской академии наук. Является автором более 300 публикаций и двадцати восьми книг, в том числе "Кибервласть: преступность, конфликты и безопасность в киберпространстве" (EPFL Press, 2013 г.); а также совместно с судьей Шольбергом – "Глобальный договор по кибербезопасности и киберпреступности – вклад в дело мира, справедливости и безопасности в киберпространстве" (Cybercrimedata, 2009 г.). Член Постоянной группы по мониторингу информационной безопасности Всемирной федерации ученых.

Дополнительная информация: www.scarg.org.

Габор Иклоди

В настоящее время Габор Иклоди работает в Службе внешнеэкономической деятельности Европейского союза (EEAS), Брюссель, в качестве Директора по вопросам кризисного управления и планирования. Ранее, являясь помощником Генерального секретаря НАТО по новым вызовам безопасности, создал и возглавил отдел НАТО по новейшей политике, занимающийся нетрадиционными вызовами, например киберзащитой, противодействием терроризму, нераспространением ОМП и энергетической безопасностью, а также ядерной политикой и стратегическим анализом. Также являлся председателем Совета НАТО по управлению киберзащитой.

До назначения на должности в международных организациях на протяжении почти тридцати лет состоял на дипломатической службе Венгрии. Его последней должностью была должность директора по вопросам политики и заместителя статс-секретаря по многосторонним вопросам и вопросам безопасности. В течение двух четырехлетних сроков занимал пост посла в скандинавских странах: вначале в Норвегии (1999–2003 гг.), а затем в Швеции (2005–2009 гг.). Большая часть его карьеры посвящена евроатлантической интеграции, многосторонней дипломатии и контролю над вооружениями.

Данил Керими

Данил Керими отвечает за формирование технологической программы, разработку глобальной стратегии по охвату общественного сектора и объединению различных инициатив, связанных с ИКТ, в рамках платформы по обеспечению гиперсоединенности (кибербезопасность, данные, технологии для человечества, ИКТ в интересах конкурентоспособности, управление использованием интернета) на Всемирном экономическом форуме (ВЭФ). Руководит привлечением ведущих руководителей государственного сектора и отраслевых организаций, экспертов общества знаний и гражданского общества к проектам Форума в области ИКТ. Кроме того, Данил отвечает за Совет глобальной программы по кибербезопасности и ежегодный глобальный отчет ВЭФ по информационным технологиям. До прихода в ВЭФ Данил занимал ряд руководящих должностей в Организации Объединенных Наций, Организации по безопасности и сотрудничеству в Европе, Международной организации по миграции и других крупных международных учреждениях.

Аксель Лехман

Аксель Лехман является почетным профессором факультета информатики Университета вооруженных сил Мюнхена, Германия, в котором до 2011 года заведовал кафедрой моделирования и имитации. В настоящее время также является исполнительным директором НИИ интеллектуальных систем (ITIS) при этом университете. Основные направления его исследований включают от компьютерного моделирования и имитации, применения систем, основанных на использовании знаний, для диагностики и поддержки принятия решений, до разработки инновационных компьютерных архитектур. Бывший президент Международного общества моделирования и имитации, член Немецкого общества информатики и Федерации азиатских обществ имитации, член редакционных коллегий различных научных журналов в области моделирования и имитации, член международных рабочих групп и групп по стандартизации, а также комитетов по оценке, например Европейского союза и НАТО. Член Постоянной группы по мониторингу информационной безопасности Всемирной федерации ученых с момента ее образования в 2001 году.

Стефан Лудерс

Стефан Лудерс, доктор философии, окончил Швейцарский федеральный технологический институт в Цюрихе и в 2002 году перешел на работу в ЦЕРН. В качестве первого разработчика системы общей безопасности, использовавшейся во всех четырех экспериментах на Большом адронном коллайдере ЦЕРН, приобрел опыт в вопросах кибербезопасности, связанных с системами управления. В дальнейшем, в 2004 году, принял на себя обязанности по обеспечению безопасности систем управления ускорителем и инфраструктурой ЦЕРН от киберугроз. Затем присоединился к Группе реагирования на инциденты в сфере компьютерной безопасности ЦЕРН и сегодня возглавляет эту группу в качестве руководителя службы компьютерной безопасности ЦЕРН, в обязанности которого входит координация всех аспектов компьютерной безопасности ЦЕРН. Сюда входит безопасность офисных вычислений, безопасность компьютерного центра, безопасность вычислений по технологии GRID и безопасность системы управления при одновременном учете операционных нужд ЦЕРН. Д-р Лудерс часто делает презентации на темы компьютерной безопасности и кибербезопасности системы управления для международных органов, правительств и компаний, а также опубликовал несколько статей по этим вопросам.

Говард А. Шмидт

В настоящее время Говард является партнером консалтинговой компании Ridge-Schmidt Cyber, занимающейся стратегическим консалтингом в области системных служб, которая помогает руководителям предприятий и правительственных органов ориентироваться в растущих потребностях кибербезопасности. Работает в этой должности вместе с Томом Риджем, первым секретарем Министерства национальной безопасности. Также является исполнительным директором Форума по обеспечению высокого качества кода программного обеспечения (SAFECode).

Обладает опытом и знаниями в областях коммерческой деятельности, обороны, разведки, правопорядка, секретности, научной деятельности и международных отношений, приобретенными более чем за 40 лет блестящей карьеры. Совсем недавно работал специальным помощником президента США и координатором по кибербезопасности Соединенных Штатов. Его прежними должностями в Белом доме являлись должности советника президентов Барака Обамы и Джорджа У. Буша по кибервопросам.

Ранее г-н Шмидт являлся президентом и главным исполнительным директором Форума по информационной безопасности (ISF). Также ранее занимал должности вице-президента, руководителя службы информационной безопасности и директора по стратегии в области безопасности компании eBay, а до этого работал руководителем службы безопасности корпорации Microsoft. Кроме того, являлся

директором по стратегии в области безопасности партнерских программ США-CERT Министерства национальной безопасности.

Г-н Шмидт имеет степень бакалавра в области делового администрирования (BSBA) и степень магистра в области организационного менеджмента (MAOM) университета Феникса. Кроме того, имеет степень почетного доктора гуманитарных наук и является почетным ассоциированным членом Киберлаборатории Карнеги-Меллона, а также почетным членом института конфиденциальности Понемона. Ранее был членом PSG в ENISA. В настоящее время профессор-исследователь в университете штата Айдахо. Член Постоянной группы по мониторингу информационной безопасности Всемирной федерации ученых.

Говард – радиооператор HAM (позывной W7HAS), пилот-любитель, турист и заядлый ездок на Харли-Дэвидсон. Он женат на Реймари Шмидт, криминалисте в отставке, исследователе и инструкторе в области компьютерной криминалистики. Вдвоем они являются гордыми родителями и счастливыми дедушкой и бабушкой.

Хамадун И. Туре

Д-р Хамадун И. Туре, Генеральный секретарь МСЭ с января 2007 года, в октябре 2010 года был переизбран на второй срок. Имеет большой опыт работы как в государственном, так и в частном секторах.

Д-р Туре, гражданин Мали, стремится превратить МСЭ в инновационную, перспективную организацию, способную решать проблемы, возникающие в стремительно изменяющейся среде ИКТ, и продолжает вести Союз к выполнению решений Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) и достижению Целей развития тысячелетия (ЦРТ).

Д-р Туре женат, имеет четырех детей и двух внуков.

Хеннинг Вегенер

Хеннинг Вегенер, бывший посол Германии. Являлся послом по вопросам разоружения в Женеве (1981–1986 гг.), помощником Генерального секретаря НАТО по политическим вопросам (1986–1991 гг.), генеральным директором Федеральной канцелярии Германии (1991–1994 гг.), а затем послом в Испании (1995–1999 гг.). Посол Вегенер был председателем Постоянной группы по мониторингу информационной безопасности с момента ее образования в 2001 году и продолжает оставаться на этой должности с коротким перерывом с 2009 по 2012 год, когда он был ее сопредседателем. Его работа была отмечена в публикациях в области внешней политики и политики безопасности, в том числе кибербезопасности. Г-н Вегенер член Римского клуба (филиал в Испании) и член советов нескольких фондов. Среди прочих степеней имеет степень доктора юридических наук Йельской школы права. henningwegener@hotmail.com

Предисловие Генерального секретаря МСЭ д-ра Хамадуна И. Туре

В этой книге рассматривается все более сложная задача укрепления доверия при использовании киберплатформ и технологий на фоне недавних резонансных инцидентов с нарушением безопасности и множества новых угроз, которые поколебали уверенность в этих важнейших средствах наших дней.

Книга является продолжением публикации "*В поисках кибермира*" 2009 года, в которой делается акцент на продвижении кибермира в сфере, которая принесла человечеству огромные выгоды и достижения, но вместе с этим породила масштабную преступную деятельность и создала новые возможности для сбора разведывательных данных, промышленного шпионажа и возникновения конфликтов.

В данном томе неизбежно вновь поднимаются вопросы, связанные с основной темой использования огромного потенциала киберпространства либо во благо, либо во вред, особенно влияния темной стороны интернета на доверие в виртуальной сфере. Вместе с тем в этой книге главной темой является продвижение концепции кибердоверия. Как отмечено во вводной главе, можно без преувеличения говорить о "кризисе доверия" в киберсфере. Более того, анализ последних тенденций свидетельствует о совпадении нескольких факторов, которые оказали совокупное негативное воздействие на кибердоверие. Среди этих факторов особую тревогу вызывают растущая милитаризация киберпространства и появление все большего количества наступательных военных средств, рассчитанных не только на военные цели, но и, за счет каскадного эффекта, на важнейшие гражданские инфраструктуры; в целях содействия преодолению этих тенденций была разработана концепция кибермира. Еще большее значение имеет небывалый уровень цифрового шпионажа и нарушения конфиденциальности в киберпространстве, который недавно стал одним из вопросов, вызывающих наибольшую обеспокоенность общества.

На протяжении всей книги авторы под разными углами зрения выявляют совокупность причин подрыва доверия, анализируют их и разрабатывают стратегии эффективного противодействия. При этом их внимание привлекают три целевых направления, которые считаются важными для восстановления и укрепления данного доверия: 1) создание *нормативной политической и регуляторной базы*, применимой конкретно к цифровому веку; 2) укрепление *способности к восстановлению,* чтобы выдерживать многочисленные случаи неправомерного использования киберпространства; и 3) обеспечение основных *свобод*, например свободы доступа и свободы выражения в рамках киберполя. Кроме того, по всем трем направлениям они выделяют и оценивают инициативы, осуществляемые на глобальном, региональном и национальных уровнях, которые способствуют достижению этих целей.

Книга представляет собой настойчивый призыв к действиям в целях решения данных вопросов и содержит веские аргументы по этому поводу. Как и в предыдущем издании, "*В поисках кибермира*", спонсорами и авторами книги являются Всемирная федерация ученых и Международный союз электросвязи, при этом обе организации находятся на переднем крае этой деятельности.

Предисловие президента Всемирной федерации ученых профессора Антонино Дзикики

В начале третьего тысячелетия наука в большей степени, чем когда-либо прежде, является основной детерминантой изменений и исторического развития. Она позволяет человечеству лучше понять, как функционирует вселенная, и еще глубже проникнуть в ее тайны. При этом сложные системы становятся все более сложными. Появляются новые формы взаимодействия между людьми и окружающей средой: взаимоотношения между разумом и компьютером претерпевают стремительные изменения и нуждаются в переоценке. Мы вступаем в новый период неожиданных открытий, а также беспрецедентных проблем.

Цифровые технологии играют важную роль в теоретической и прикладной науке. Эти технологии и средства на их основе получают все более широкое распространение, создавая кривую роста и доступности знаний, которую практически невозможно представить, а также обеспечивая устройства контроля и системы управления, которые используются практически во всех сферах человеческой деятельности. Специализированные компьютерные приложения, распределенные вычисления с использованием технологий GRID и облачных вычислений, основанные на высокоразвитых информационных инфраструктурах, развитие микроэлектроники и новых датчиков, развивающийся мир взаимных соединений огромного количества цифровых устройств, нередко осуществляемых автоматически, а также быстрые преобразования производственных процессов – вот лишь некоторые характерные черты этого нового века.

Но я вовсе не собираюсь перечислять все бесчисленные преимущества и возможности цифрового века. Как президент Всемирной федерации ученых, я хотел бы подчеркнуть значение науки и развития цифровых технологий для содействия делу мира и преодоления чрезвычайных ситуаций глобального масштаба. Эффективный мониторинг этих чрезвычайных ситуаций зависит от подбора информации в реальном времени – в интересах предотвращения, реагирования, восстановления и исправления. И я отчетливо сознаю моральную ответственность ученого, связанную со всеми этими проблемами.

Цифровое пространство не знает границ. Его повсеместная распространенность сделала мир плоским и резко сократила расстояние и время. Кибертехнологиям, как и всем современным технологиями, присуща двойственность – они могут

использоваться во благо или причинять зло и при этом в глобальных масштабах. Киберпространство – это область огромных возможностей, но также и опасностей, усиленных отсутствием приемлемой нормативно-правовой базы всеобщего действия. Враждебное использование цифровых технологий представляет все большую угрозу, и поэтому кибербезопасность и защита данных становятся все более важными базовыми компонентами управления цифровыми рисками. Они стали основными аспектами цифровой революции, и должны стать действительно быстрорастущей отраслью, чтобы преодолеть опасные тенденции.

Всемирная федерация ученых в рамках своей межотраслевой группы по информационной безопасности более десяти лет участвует в этой деятельности. В предыдущей совместной публикации с Генеральным секретарем МСЭ упор делался на защищенном и мирном использовании цифровой технологии – на поиске кибермира. Этот том касается еще одного важного аспекта функционирования цифрового общества: доверительных отношений, доверия. Пользователи и общество в целом должны быть не только уверены в том, что технология исправно функционирует, но и должны доверять целостности и конфиденциальности цифровых устройств и данных, а также базовых сетевых структур. В основе любого целенаправленного и прочного сотрудничества лежит взаимное доверие. Оно имеет решающее значение в глобальном киберпространстве, во все более взаимосвязанном глобальном информационном обществе. Доверительные отношения делают международное взаимодействие более эффективным и продуктивным благодаря оправданию взаимных ожиданий доброй воли и взаимности. Я признателен Генеральному секретарю Туре и соавторам этого тома за изложение многих аспектов кибердоверия и за формулирование необходимых рекомендаций.

Введение: Кризис кибердоверия

Хеннинг Вегенер

Три года назад Генеральный секретарь МСЭ и члены Постоянной группы по мониторингу информационной безопасности Всемирной федерации ученых опубликовали книгу "*В поисках кибермира*"[1]. В данной книге заостряется внимание на растущих опасностях киберпространстве и призываются к действиям все заинтересованные стороны в рамках киберполя с целью участия в коллективных мерах по обеспечению приемлемого уровня стабильности в интернете и структурах цифровых сетей, а также продвижения концепции глобального кибермира. Данная

[1] *В поисках кибермира*, Международный союз электросвязи и Всемирная федерация ученых, Женева, январь 2011 г.

книга, которая намеренно сделана лаконичной и отражает более широкую современную общественную дискуссию, не устарела. Ее авторы, многие из которых являются и авторами нынешнего продолжения, придерживаются результатов своих исследований и рекомендаций, сделанных в то время.

Однако с тех пор ситуация стала более тревожной, и можно без преувеличения говорить о новом факторе угроз в киберпространстве, получающем дальнейшее развитие на наших глазах. В более ранней публикации в центре внимания были, в основном, тревожные перспективы киберконфликтов, включая кибервойну. Можно сказать, что данная перспектива стала вызывать еще большую обеспокоенность, и совершенно не ослабевает. Поэтому нет ничего удивительного в том, что киберконфликты занимают важное место в этой публикации; соответственно, между двумя названиями есть четкая преемственность. Вместе с тем, в вошедших в этот том статьях акцент сместился соразмерно развитию угрозы. Главной темой настоящей книги является концепция кибердоверия, при этом ставится цель проанализировать тенденции, подорвавшие его до столь опасного уровня, а также стратегии и методы, необходимые для его восстановления[2].

Идея о том, что доверие является необходимым условием функционирования информационного общества, основанного на цифровых технологиях, не нова. При внимательном изучении документов, принятых Всемирной встречей на высшем уровне по вопросам информационного общества (ВВУИО) на ее двух сессиях в 2003 и 2005 годах, сразу становится ясно, что концепции доверительных отношений и доверия проходят красной нитью через ее тексты и рекомендации. Например, "доверие и безопасность относятся к главным опорам информационного общества", а "укрепление доверия и безопасности" также является основной задачей Направления деятельности 5 ВВУИО.

В рамках проводимых после ВВУИО обсуждений, в Отчете содействующих организаций по этому направлению деятельности за 2014 год в качестве одного из основных проблемных вопросов указано (выдержка из резюме отчета): "важнейшей задачей является укрепление основы для доверия: повышение уровня доверия к цифровым устройствам, кибербезопасности и создание доверительной среды между государственными и частными организациями. Уровень доверия граждан к цифровым услугам и интернету должен быть улучшен"[3].

---

[2] Название книги "*В поисках кибердоверия*" выбрано таким образом, чтобы показать преемственность между двумя публикациями. Однако в каждом из двух случаев слово "поиск" используется по-разному. В первой книге оно выражает стремление к состоянию мира, который еще не достигнут, а во второй книге – доверие имеется, но оно резко ослаблено, и слово "поиск" означает намерение его восстановить и укрепить.

[3] Документ WSIS+10/4/2.

Доверие является основным элементом информационного общества, и поэтому его актуальность для всех сегментов цифрового мира очевидна. Таким образом, хотя в книге "*В поисках кибермира*" акцентируется внимание на других вопросах, в ней содержатся развернутые рассуждения относительно концепции доверия и его всеохватывающей роли в обществе[4]. Автор подчеркивает, что "доверие и надежность … лежат в основе человеческого существования". Они поддерживают все социальные контакты и позволяют людям справиться с высоким уровнем неопределенности и сложности современной жизни, уменьшая тем самым осознаваемый риск. В проведенном им анализе содержится обзор современной литературы по этой главной концепции социальной жизни. Книга по-прежнему доступна для широкого ознакомления, и поэтому общей ссылки на исследование автора может быть достаточно[5].

Доверительные отношения и доверие во многом синонимы, однако доверительные отношения относятся в большей степени к межличностным отношениям, а доверие скорее к отношениям между человеком и объектами или институтами, не принадлежащими к человеческому роду. Применительно к нашей теме доверие включает доверие к цифровым устройствам и продуктам с точки зрения программного и аппаратного обеспечения, сетей, инфраструктур, приложений и процедур обработки. Поэтому в данной публикации в качестве основного термина выбрано "доверие", при этом обращается внимание на личные ожидания и восприятия, связанные с термином "доверительные отношения".

Как уже было указано, доверие является необходимым условием функционирования цифрового мира. Однако последние события, затронувшие этот непрерывно растущий цифровой мир, серьезно поколебали доверие. Поэтому можно без преувеличения говорить о кризисе кибердоверия.

Сочетание факторов, которые создают и подпитывают кризис, очевидно, и их можно легко перечислить.

- Растущая обеспокоенность в связи с тем, что киберпространство становится милитаризованным, что все больше государств разрабатывают наступательные военные средства, рассчитанные не только на военные цели, но фактически на важнейшие гражданские инфраструктуры и образ жизни гражданского населения противника, приводящие к неуправляемым побочным эффектам, и что отсутствуют факторы, сдерживающие участие в цифровой гонке вооружений. В настоящее время более 100 государств наращивают свои возможности по осуществлению цифровых атак в

---

4 Жак Бус, Необходимость доверия: Понятие доверия и его роль в обществе, *В поисках кибермира*, стр. 17.

5 Основными цитируемыми авторами являются О'Хара, Луманн, Хардин и Фукуяма.

необузданном и все более опасном стихийном состязании по обеспечению стратегической взаимности, при котором в соответствующих документах прямо заявляется о злонамеренном использовании возможностей ИКТ как средстве достижения военно-политических целей. Эти опасения не препятствуют обоснованной необходимости в самообороне.

- Несмотря на необходимость в первоочередной адаптации международного права к реалиям цифрового века и определении пределов враждебного использования цифровых технологий, растет обеспокоенность, что вместо содействия кибермиру существующие усилия по разработке таких нормативных инструментов в действительности узаконят масштабное пополнение военных арсеналов государств кибероружием, сделав их оперативное развертывание обычной составляющей стратегического планирования.
- Растущие опасения, что гражданские инфраструктуры, имеющие жизненно важное значение, будут подвергаться атакам государств и негосударственных субъектов, будь то под предлогом законных военных мероприятий или с преступными намерениями.
- Неопределенность в отношении правил и поведенческих норм, которые могли бы применяться ко всем этим обстоятельствам и содержать показатели и признаки, способствующие предотвращению потерь и восстановлению кибердоверия. Эта неопределенность дополнительно повышается из-за неудачных нормотворческих усилий по созданию универсальных согласованных кодексов достаточно широкого применения, предпринятых за прошедшее десятилетие.
- Еще более сложная техническая среда, обладающая огромным потенциалом, но и сопряженная с новыми уязвимостями и непредсказуемыми последствиями для множества взаимных соединений. Опасения усиливаются из-за стремительного роста количества цифровых устройств; дополнительные уязвимости за счет расширения "применения" цифровых пользователей; проблемы безопасности, вызванные переходом на мобильные и облачные приложения; тревожащий рост новых компонентов вредоносного программного обеспечения[6]; восходящая кривая инцидентов, связанных с киберпреступлениями, которые сопряжены с колоссальными затратами для национальных экономик, корпораций и индивидуальных цифровых

6 На момент написания данной статьи наглядной демонстрацией все более коротких промежутков времени, в течение которых обнаруживаются крупные уязвимости и возникают новые угрозы, стал вирус Shellshock, описанный как "совершенно серьезный" и предположительно поставивший под угрозу более 500 миллионов компьютеров, который появился вскоре после сообщения об ошибке Heartbleed в апреле 2014 года.

пользователей; и появление еще более могущественных преступных синдикатов, действующих в международном масштабе, которые готовы и способны участвовать в киберпреступлениях и киберконфликтах по найму. Как указано выше, совокупность этих обстоятельств представляет новый фактор, если не качественный скачок киберугроз, способный еще больше подорвать кибердоверие.

- Постоянная неопределенность с управлением использованием интернета, поднимающая соответствующие вопросы о возможности обеспечения "глобальной, функционально совместимой, способной к восстановлению, стабильной, децентрализованной, безопасной и взаимосвязанной сети, доступной для всех"[7].
- Внушающая растущую обеспокоенность проблема реализации прав человека в сети, вызванная массовым правительственным цензурированием доступа и контента (киберрепрессии) во все большем числе стран.
- Возможно, наиболее важное и остро актуальное в настоящий момент новое явление заключается в несдерживаемом, неограниченном и технически неуправляемом несанкционированном доступе к цифровым системам через поиск по большим данным. Это привело к небывалому уровню цифрового промышленного шпионажа и беспрепятственной, нередко, по-видимому, необоснованной массовой слежке разведслужб некоторых государств, выходящей за рамки их национальных полномочий и беззастенчиво ущемляющей суверенитет и нарушающей правопорядок других государств[8].

Несомненно, восстановление доверия является проблемой, на которую должны реагировать все заинтересованные стороны в цифровом мире, и хочется надеяться, что данная публикация может внести вклад в этом направлении, совместно с другими учреждениями и организациями, преследующими ту же цель – восстановить доверие совместными взвешенными усилиями[9].

Изложенный в данной книге подход к решению рассматриваемой задачи сосредоточен на трех проблемных областях, непосредственно относящихся к

---

7 Многостороннее заявление NETmundial от 24 апреля 2014 года.

8 О важности доверия в этом отношении см. Leif-Eric Easley, *Spying on Allies,* SURVIVAL, том 56, № 4, август-сентябрь 2014 г., стр. 141.

9 Тема доверия также прозвучала на недавних международных конференциях, привлекших большое внимание, таких как Второй саммит по кибербезопасности, организованный Мюнхенской конференцией по безопасности и компанией Deutsche Telekom, Бонн, ноябрь 2013 года, на которой Говард А. Шмитд, один из авторов данной публикации, принял участие и сделал основной доклад.

укреплению кибердоверия, – теме, которая в настоящее время широко и повсеместно обсуждается общественностью.

Знакомясь с тремя главами книги, читатель должен иметь ввиду, что данная публикация не является учебником, научным трудом, призванным полностью охватить эту сложную тему, и в ней также не ставится цель отразить единую общепринятую позицию по всем тематическим аспектам. Наоборот, публикация структурирована таким образом, что в ней объединены разные тексты, написанные МСЭ, и документы, подписанные членами Всемирной конфедерации ученых, в которых отражены их личные мнения. Следует подчеркнуть, что не считая официального уведомления и правовой оговорки, содержащихся в начале книги, редакторы сознательно поощряли представление широкой палитры взглядов, чтобы обогатить дискуссию и при этом обеспечить общую совместимость мнений.

Первая часть отражает стремление к более комплексной нормативной базе с целью регулирования поведения в киберпространстве и придания ему более предсказуемого и надежного характера. Она посвящена международным усилиям, направленным на выработку, принятие и осуществление на практике мер по укреплению доверия и согласованных кодексов поведения для совершенствования доверительных отношений – как это делают другие, более широкие правовые инструменты, способствующие повышению кибердоверия – в виде согласованных правовых предписаний и совместного международного контроля за их исполнением. Цель заключается в том, чтобы наметить дальнейшие шаги по постепенному, но стабильному достижению консенсуса в нормативной сфере на международном и национальном уровнях.

Во второй части делается акцент на киберзащите и способности цифровых систем выдерживать атаки и конфликты, а также на способах уменьшения уязвимости, смягчения или сведения на нет последствий атак, или восстановления возможностей систем, которым причинен ущерб в результате атаки, или работа которых нарушена из-за неисправностей, ошибок и отказов киберсреды. Ключевым термином является способность к восстановлению[10]. После анализа существующих и ожидаемых угроз в этой главе раскрывается широкий спектр методов и стратегий, совместное использование которых может изменить баланс сил в пользу успешной защиты в давнем состязании между средствами атаки и защиты, которое столь стремительно разворачивается на наших глазах в современном цифровом мире.

---

[10] Способность к восстановлению, т. е. способность противостоять неблагоприятным факторам, продолжать работу и восстанавливаться, означает больше, чем сочетание взаимодействующих технических исправлений. Этот термин также подразумевает общую устойчивость – в противоположность уязвимости – всей системы в долгосрочной перспективе. См. Dhruva Jaishankar, *Resilience and the Future Balance of Power,* Survival, том 56, стр. 217, июнь-июль 2014 года.

Заключительная глава посвящена теме баланса между свободой в интернете – и в рамках всех прочих видов цифровой связи – и предписываемым государством вмешательством: баланс между цифровой конфиденциальностью и безопасностью государства. Справедлив ли тезис "конфиденциальности более не существует", учитывая огромное, практически неограниченное, число технических средств, дающих возможность безнаказанно отслеживать любые частные и корпоративные линии связи и хранилища данных? В этой главе предпринята попытка прояснить масштаб законного надзора, осуществляемого зарубежными и национальными службами разведки, и правовую основу, в особенности в части, касающейся тех стран, которые не организуют такого надзора, допускающую разрешение этого направления деятельности. В главе исследуются также имеющиеся возможные санкции против такой чрезмерной деятельности. Цель главы, таким образом, заключается в том, чтобы внести вклад в процесс принятия имеющей обязательную силу согласованной нормативно-правовой базы, которая уравновешивает законные интересы безопасности и основные права, действительность законодательства государства, обеспечивающего защиту данных и безопасность данных, и базовый принцип свободы в интернете. Этот животрепещущий вопрос, также как вопрос незаконной государственной цензуры интернета, требует всестороннего обсуждения в международной перспективе.

И очевидно общая цель этого трехстороннего дискурса заключается в предупреждении дальнейшего ослабления кибердоверия и его эффективном и прочном восстановлении. Этот кризис кибердоверия должен быть преодолен.

Глава I: Кибернормы

Введение

В этой главе представлен обзор проблем и предпринимаемых в настоящее время усилий, направленных на определение комплекса норм, принципов и образцов передового опыта в области кибербезопасности на международном уровне. Возникающие угрозы – от шпионажа до подобных военным атак, а также предполагающий участие многих заинтересованных сторон, транснациональный и технический характер интернета формирует для государств необычное поле деятельности в киберпространстве: национальные правительства имеют дело с доменом, над которым они не осуществляют, как правило, прямого контроля, но в связи с которым им все чаще приходится защищать своих граждан, в особенности по вопросам их прав человека. В настоящее время предпринимаются комплексные региональные меры и ограниченное число глобальных мер по установлению общих базовых норм, которые позволят получать такую защиту.

Информационно-коммуникационные технологии (ИКТ) все в большей степени становятся повсеместно распространенными, и их использование экспоненциально растет как в развитых, так и в развивающихся странах. Конгломерат безопасных и вызывающих доверие ИКТ – необходимое условие доверия при их расширяющемся использовании. Однако в настоящее время сложился ряд тенденций, подрывающих это доверие:

- широкомасштабный шпионаж в целях национальной безопасности, которому способствует резкое падение стоимости сбора и хранения личной информации;
- использование компьютерных кодов для действий военного характера, выходящих за пределы национальных границ;
- существование внешне необузданной и эклектичной группы мошенников – от наемных спамеров до разработчиков ботнетов по найму;
- и сложность привлечения к ответственности киберпреступников, находящихся за пределами юрисдикции, к которой относится атакуемая система.

Эффективное реагирование на эти сложные вопросы требует региональной кооперации. В настоящей главе представлена предпринимаемая в этом направлении деятельность, в том числе предпринимаемая в рамках системы Организации Объединенных Наций (ООН) и другими межгосударственными органами, а также некоторые базовые рекомендации, касающиеся глобального соглашения по кибербезопасности. Основу этих инициатив составляют меры по укреплению доверия (СВМ) – этот термин вошел в обиход в эпоху холодной войны.

Глава подразделяется на четыре раздела. В первом разделе подчеркивается необходимость участия государств в СВМ, обусловливаемые этими мерами задачи и потенциальные преимущества. Далее в главе освещается принятый в ООН подход к выработке норм, правил и принципов, относящихся к кибербезопасности, в том числе принципов и рекомендаций, рассчитанных на перспективу, а также применимость международного права к ИКТ. В третьем разделе эта тема рассматриваться более подробно, представлен обзор сходных черт киберпространства и деятельности и участников деятельности, осуществляемой в киберпространстве, и других доменов военных действий и шпионажа, а также широкий комплекс руководящих указаний по разработке глобального, подобного договору, инструмента кибербезопасности. В заключение, в четвертом разделе представлена концепция безопасности, принятая в ООН, и особое внимание уделено внедренным и ожидаемым механизмам специализированных учреждений и долговременным перспективам роли международной системы в области кибербезопасности и киберпреступности.

Было бы заманчивым, и во многих аспектах даже представляется необходимым, включить еще один раздел – об управлении интернетом, поскольку в настоящей публикации показано, что имеющиеся сомнения относительно будущего интернета

входят в число очевидных причин снижения кибердоверия. Однако ведущиеся на международном уровне дискуссии по вопросу управления, в которых еще не найдены пути согласования различающихся государственных позиций, затрудняют для МСЭ выработку твердых мнений. Вместе с тем можно отметить с удовлетворением, что дебаты, результатом которых стало недавнее согласование Многостороннего заявления о будущем управлении интернетом (NETmundial), принятого на конференции NETmundial, состоявшейся в Бразилии в апреле 2014 года, обеспечили ощутимый прогресс, и что, несмотря на намеренное придание этому документу необязательной силы, очевиден зарождающийся общемировой консенсус по ряду основных принципиальных вопросов. Соответствуя своему глобальному предназначению, МСЭ может безусловно поддержать все усилия, направленные на сохранение интернета как "глобальной, функционально совместимой, способной к восстановлению, стабильной, децентрализованной, безопасной и взаимосвязанной сети, доступной для всех" в форме единого нефрагментированного пространства. Аналогичным образом МСЭ может поддерживать содержащееся в заявлении конференции NETmundial утверждение о том, что "массовое и произвольное слежение подрывает доверие к интернету и доверие к экосистеме управления интернетом".

1.1 Роль СВМ в обновленной концепции международной кибербезопасности: перспективы глобального реагирования и международного договора

Соланж Гернаути

Насущная потребность в кибердоверии

Всего за нескольких лет интернет превратился во всепроникающий и практически неотъемлемый элемент нашей повседневной деятельности. Цунами под названием "интернет" накрыло всех без исключения. Умные устройства делают все большее число услуг нематериальными, это включает услуги здравоохранения и медицинские услуги, парадигму облачных вычислений, интернет вещей, к которому мы движемся, а также идею о том, чтобы привыкнуть к постоянному подсоединению и зависимости от ИКТ. Интернет сегодня можно рассматривать как некий цифровой протез и киберпространство, являющиеся "естественным" расширением нашей окружающей среды. Как фактор перемен и цивилизации, интернет формирует структуру информационного общества, в процессе построения которого – во всемирном масштабе – мы находимся. Интернет составляет часть непрерывного процесса эволюции и создаваемых человеком инноваций, которые творят нашу историю.

Внедрение цифровых технологий глубоко и навсегда изменили способы нашего общения, поведения, мышления, действия, обучения, ведения коммерческой деятельности, влияния, дестабилизации и нанесения ущерба и даже слежения,

ведения войн и поддержания общественного порядка. Технология, таким образом, не является нейтральной, так как несет существенные структурные изменения, затрагивающие нас напрямую.

Все используют один и тот же интернет для частных, личных и профессиональных приложений, для здравоохранения, обеспечения энергией, цепочек поставок, культуры и даже безопасности. Следовательно, использование интернета – от развлечений до мира финансов, а также для всех систем управления критически важной инфраструктурой, информацией и электросвязью – становится неизбежным.

Интернет и совокупность основанных на нем инструментов ускорили технологическую зависимость и нашего общества, и, в определенной степени, отдельного человека. Мы создаем и обрабатываем возрастающие объемы информации, трафика, взаимодействия. Мы потребляем все больше информации, компьютерных ресурсов и энергии, вследствие чего создается еще больше информационных отходов.

Таким образом информационные технологии становятся объединяющим фактором для всех дисциплин и памятью нашего наследия (цифровое культурное достояние, цифровое наследство бизнеса и отдельных людей). Без информационных технологий более невозможны знания и наука. Не следует также забывать, что великие основополагающие принципы нашего общества, такие как демократия, личная идентичность и суверенитет государств, также в определенной степени зависят от информационных технологий или могут быть нарушены в результате их неправомерного использования или захвата.

Напомним о той роли, которую социальные сети и широкий диапазон инструментов связи на базе интернета могут играть в стратегиях влияния, независимо от того, используются ли они государствами, лоббистскими кругами или преступными и террористическими группировками. Используемый для разрушения репутаций, влияния на людей, группы и лидеров, распространения дезинформации и манипулирования мнениями, интернет становится полем битвы за ценную информацию. В то же время информационные технологии открывают перед преследующими злонамеренные цели и преступными организациями возможность повышения своей эффективности, давая выход своим беспредельным и безнравственным фантазиям и ведя новые виды войн в киберпространстве, включая информационную войну. Отказ признать эту реальность означает неоправданно подвергать себя опасности потенциальной потери экономической конкурентоспособности, стабильности, национального суверенитета и международного доверия. СМИ, а также профильные специалисты сообщают о бесконечной череде случаев крупномасштабных краж данных на предприятиях, успешных кибератак или захвате информационных ресурсов с целью получения выкупа.

Кибербезопасность доверия приобретает, таким образом, огромное значение не только в отношении инфраструктуры ИКТ, предоставляемых услуг и обрабатываемой ими информации, но и в отношении их безопасности.

Киберпространство не только повышает уровень сложности, но изменяет концепцию подлежащих защите территорий

Сегодняшний мир – это сложный глобализованный мир, в первую очередь характеризующийся интенсивным использованием устройств, инфраструктуры и услуг ИКТ. Зависимость и взаимозависимость имеющих важнейшее значение объектов инфраструктуры и инфраструктуры ИКТ привели к появлению новых уязвимостей общества. Это повысило уровень сложности методов обеспечения безопасности, защиты и охраны жизненно важной для нас деятельности, осуществляемой на политическом, экономическом, социальном и индивидуальном уровнях. Кроме того, взаимозависимость рисков ослабляет общую основу способности к восстановлению как на национальном, так и на международном уровне. Кибербезопасность, независимо от того, употребляем ли мы этот термин или называем ее информационной безопасностью или цифровой безопасностью, становится важнейшим вопросом на современном этапе как следствие обеспокоенности, обусловливаемой политическими, экономическими, юридическими вопросами и технологиями. Именно это определяет важнейшее значение управления кибербезопасностью и сложность различных элементов, используемых при поиске решений, удовлетворяющих требования безопасности.

Киберпространство – это являющаяся одновременно и виртуальной и реальной область, которую составляют базирующиеся на интернете технологии, услуги и данные. Оно стало, по крайней мере для молодых поколений, такой же частью естественного ландшафта, как и суша, море, атмосфера и космос, столь же обычной, как для нас электричество. Некоторые рассматривают киберпространство как динамичную территорию, которая находится в постоянном развитии, или как территорию, которую необходимо завоевать, подчинить или контролировать. Другие же видят ее как область, в которой можно выражать или проявлять силу, или как источник законного или незаконного личного или экономического обогащения либо как цитадель свободы, либо как поле битвы. В реальности же это в разной степени и в разной мере одновременное сочетание всех этих аспектов. В целом оно отражает наши политические, экономические и социальные реалии, и ни в чем не лучше и не хуже них. Оно является свидетельством реальности глобализации, часть которой – технико-экономическая унификация.

В гиперсвязанном мире с трудом поддается определению концепция территории, но это также справедливо в отношении безопасности и защиты цифровых территорий. Традиционная трактовка безопасности более неприменима. Реализации защиты по периметру для изоляции информационной среды стала невозможной в результате эволюции технологий (мобильная передача данных, умные устройства и облако) и их

использования (социальные сети, электронные платежи и т. п.). Введение криптографических решений часто действует как тормоз интеграции услуг, простоты использования и обеспечения приемлемых показателей работы. Криптография по-прежнему используется в недостаточной степени, и доверие к криптографическим решениям остается на низком уровне. Дело, названное "Heartbleed"[11], в апреле 2014 года выявило крупный дефект безопасности в одном из наиболее широко использовавшихся решений, интегрированных в веб-сервисы. В очередной раз общественность узнала об уязвимостях в услугах, предназначенных для укрепления надежности инфраструктуры и безопасности электронных транзакций.

Хрупкость доверия

В мире интернета отдельные люди, организации и государства сталкиваются с ранее неизвестными киберугрозами и новыми рисками. Киберпространство является пространством сбоев, нарушений функционирования, а также киберпреступности и киберагресии. Киберугрозы все еще слишком часто не распознаются в достаточной степени и недопонимаются, вследствие чего легко порождают страх. Мы не можем безусловно предсказать, когда и как эти угрозы станут реальностью, или эффект домино и ту цепочку событий, которые они вызовут, или же идентифицировать их авторов и людей, стоящих за ними.

Мы теперь знаем наверняка, по таким делам как, в первую очередь, WikiLeaks (2010)[12] и Prism (2013)[13], что цифровой секретности не существует и что за нами постоянно ведется тщательный электронный контроль и отслеживание, слежка, наблюдение и мониторинг. Мы должны понимать, что наблюдение за нами ведется в крупных масштабах и что мы активно участвуем в этом, используя определенные веб-услуги и мобильные телефоны. Мы не можем долее оставаться в неведении о том, что наши личные данные, поведение, вкусы и связи создают основу экономических моделей, которые приняты большинством поставщиков так называемых бесплатных услуг, и что эта информация весьма востребована.

В наши дни возможности мониторинга, которые обеспечивают информационные технологии и их поставщики, вызывают глобальный кризис доверия и к этим технологиям, и к основным участникам этого сектора. Мы все больше узнаем о хрупкости цифровой среды, о хрупкости доверия к технологиям и участникам сферы кибербезопасности.

---

11 https://www.schneier.com/blog/archives/2014/04/heartbleed.html

12 http://www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points

13 http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

Формирование доверия к инфраструктуре ИКТ требует разрешения и преодоления трудностей на нескольких уровнях, а именно:

- трудность для отдельных лиц, организаций и органов власти понимать угрозы, выявлять риски и принимать эффективные и действенные меры по снижению рисков, в том числе трудности в разблокировании достаточных инструментов для борьбы с киберпреступностью;
- трудность предупреждения злоупотреблений и превышений в киберпространстве и ликвидации последствий инцидентов и даже кризисов, которые могут возникать в результате;
- трудность обеспечения защиты граждан, потребителей, детей, нашего цифрового наследия и наших секретов;
- но также и трудности выражения наших потребностей в кибербезопасности и установлении прав и обязанностей участников и обеспечении их соблюдения.

Не только признать трудности и недостаточность, но и определить реальные потребности

Кибермир принес новые уязвимости и расширил диапазон угроз, которые могут их использовать. Об этом нам ежедневно напоминают в новостях, сообщая о таких случаях, как кражи данных, утрата контроля, захват информационных ресурсов с целью получения выкупа, взлом почтовых учетных записей, мошенничество всевозможных видов, обман доверия. Термины "хакер" или "аноним" сегодня стали обыденными, а кибервредоностность стала реальностью для всех пользователей интернета.

Нам необходимо признать:

- недостаточность современных мер безопасности;
- недостаточность устойчивости нашей инфраструктуры и нашей способности справляться со сложными кризисами, которые могут возникать;
- недостаточность информационно-просветительских мер, принимаемых как в интересах широких слоев населения, так и в рамках образовательных структур – от начальной школы до высшего учебного заведения, включая обучение на протяжении всей жизни, и недостаточность исследований в целях разработки "национальных" решений;
- недостаточность киберкомпетенции и людских ресурсов в каждом домене и в каждой области деятельности;
- недостаточность технических средств, предоставленных судебным системам и полиции для противодействия расширению киберделиквентности и киберпреступности.

Мы должны также подчеркнуть недостаточность знаний и междисциплинарного, глобального, системного и всестороннего подходов к управлению киберрисками, недостаточность национального и международного сотрудничества и взаимодействия, недостаточность судебной помощи, а также недостаточность партнерств государственного и частного секторов, гражданского и военного доменов.

Я представила идеи хрупкости, трудности и недостаточности, и все они коррелируются с идеей сложности. Эта идея означает сложность работы с политическим, дипломатическим, экономическим, управленческим, судебным, а также с технологическим и людским аспектами, с тем чтобы обеспечить учет всех рисков. Сегодня мы знаем, что информационное общество должно основываться на мерах доверия и безопасности, что наблюдение не является синонимом безопасности и что безопасность требует надежных мер мониторинга, соответствующих надлежащей правовой системе, а не вводимых технологиями, поставщиками или наиболее сильными участниками. Следует также определить пределы технологической глобализации и технологического империализма.

Существует необходимость понять, что киберриски приобретают характер планетарной чрезвычайной ситуации, усиливая все традиционные риски, связанные, например, с ядерными установками, загрязнением или терроризмом, и что существует вследствие этого **необходимость** действовать. Главным образом, должно быть обеспечено личное и коллективное участие и разработаны и предоставлены инструменты, которые позволят отвечать на вызовы безопасности двадцать первого века.

Таким образом, существует реальная настоятельная потребность в высвобождении ресурсов и введении организационных структур и специальных процедур на всех уровнях – кантональном, региональном, национальном и международном, с тем чтобы усилить преимущества, предоставляемые информационными технологиями, и выгоды появления новых возможностей, которые они открывают. Одновременно с этим следует сокращать недостатки, в первую очередь в целях обеспечения национальной конкурентоспособности и экономической безопасности, от которых зависит благополучие всех нас.

Неотложная потребность в международном документе

Киберпространство, если мы рассматриваем его как пятое общее измерение наряду с сушей, воздухом, морем и космосом, обусловливает неотложную потребность в координации и сотрудничестве между всеми странами, точно также как это происходит в отношении четырех других измерений.

Мы уверены, что существует реальная и неотложная потребность в международном соглашении для принятия последовательного и глобального подхода к решению проблемы незащищенности киберпространства. Организации, предприятия и государства сталкиваются со значительными рисками ненадлежащего раскрытия,

неправомерного присвоения и уничтожения данных и информации. Такие инциденты, анализируемые на макроскопическом уровне, могут рассматриваться как создающие потенциальную угрозу не только конкурентоспособности или репутации коммерческого предприятия, но и общественной безопасности, защите и самой демократии на национальном уровне.

Если мы уверены в том, что киберпространство может во все большей степени восприниматься как глобальное экономическое и военное поле битвы, где возможно развертывание киберконфликтов, отражающих все виды политической и экономической конкуренции, то настало время оговорить, что приемлемо, и что неприемлемо на общей и утвержденной основе, и предложить эффективный международный документ для контроля над этим измерением. В отсутствие общего понимания и международных соглашений невозможно будет разрабатывать эффективные меры безопасности для надлежащей защиты ресурсов ИКТ (включая имеющую важнейшее значение информацию и жизненно необходимую инфраструктуру), борьбы с киберпреступлениями и сохранения основных прав человека. Это требует глубокой приверженности всех соответствующих участников и заинтересованных сторон на национальном и международном уровнях.

Национальные и международные стратегии должны существовать не только для реагирования на кибератаки, то есть определяя ответные меры, но должны также предусматривать упреждающие меры, позволяющие не допускать нарушений систем безопасности и предупреждать нежелательные инциденты. Это возможно осуществить, например путем формирования надлежащей культуры кибербезопасности, сокращая уязвимости, которые могут использоваться для атак на системы. Учитывая системным образом все факторы, которые могут привести среди прочего к девиантному поведению, кризисам, актам мести или преступлениям, наращивая уровень компетентности и усиливая последовательные меры в рамках всестороннего и глобального подхода.

Эти вопросы невозможно эффективно разрешать исключительно на местном уровне. Аналогично тому, как Киотский протокол[14] является международным соглашением, увязанным с Рамочной конвенцией ООН об изменении климата, Глобальный протокол по кибербезопасности и киберпреступности должен стать действительно универсальным подходом к снижению рисков и угроз в киберпространстве. Он должен обеспечивать необходимую архитектуру для введения эффективных национальных и международных мер противодействия кибератакам и должен включать четкое определение приемлемого и неприемлемого поведения, а также необходимые модели управления.

---

[14] http://unfccc.int/essential_background/kyoto_protocol/items/1678.php

Содействие международному диалогу

Напомним для сведения, что в мае 2007 года МСЭ начал осуществление Глобальной программы кибербезопасности (ГПК)[15], которая является платформой для координации международного реагирования на растущие вызовы кибербезопасности. В помощь МСЭ при разработке этого стратегического предложения была создана Группа экспертов высокого уровня (HLEG). Члены HLEG были выдвинуты Генеральным секретарем МСЭ при должном учете географического разнообразия и компетентности для обеспечения представленности многих заинтересованных сторон. В состав HLEG входят более ста всемирно известных специалистов, обладающих специальными знаниями в самых разных областях[16]. В их числе представители администраций МСЭ, Государств-Членов, отрасли, региональных и международных организаций, а также исследовательских институтов и академических организаций[17]. В ноябре 2008 года был подготовлен Глобальный стратегический отчет[18], выпущенный МСЭ[19]. В Отчете представлены стратегии в пяти областях работы: правовые меры, технические и процедурные меры, организационные структуры, создание потенциала и международное сотрудничество. ГПК обеспечивает необходимую архитектуру для выработки эффективных национальных и международных мер, побуждающих страны разрабатывать национальные программы кибербезопасности и осуществлять международное сотрудничество. Это следует рассматривать как важный первый шаг к формированию глобального подхода к кибербезопасности. С тех пор во всем мире ведется широкий диалог по проблеме кибербезопасности[20].

---

15 http://www.itu.int/osg/csd/cybersecurity/gca/index.html

16 http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html

17 Судья Штайн Шольберг из Норвегии был председателем HLEG, а Соланж Гернаути – одним из руководителей по направлениям "Организационные структуры" и "Создание потенциала", соответственно.

18 Кроме того, в 2008 году МСЭ создал Международное многостороннее партнерство против киберугроз (ИМПАКТ), международную инициативу с участием государственного и частного секторов, направленную на расширение потенциала мирового сообщества по предупреждению киберугроз, защиты от киберугроз и реагированию на них (www.itu.int/osg/csd/cybersecurity/gca/impact_index.html).

19 http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

20 Подробную информацию можно найти в публикации "The baseline review ICT-related process and events, Implications for international and regional security", ICT for Peace Foundation. См.: http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security.

После длительного периода международного сотрудничества[21] было сформулировано предложение для документа "Глобальный договор по кибербезопасности и киберпреступности – вклад в дело мира, справедливости и безопасности в киберпространстве".

К глобальному документу в интересах глобального сообщества

В интересах содействия удовлетворению ставшей уже универсальной потребности в управлении киберрисками и борьбе с глобальными кибератаками, киберпреступностью и создающим опасность или ненадлежащим использованием интернета мы нацелены на определение потребности в обновленной концепции международной кибербезопасности на основе эффективного международного диалога и соглашений. Осуществляя это, мы стремимся внести вклад в обеспечение чуть большего мира, справедливости и безопасности в киберпространстве и, следовательно, в физическом мире. Это может привести к созданию Глобального договора или свода договоров, касающихся киберпространства.

Такой глобальный договор или свод договоров по кибербезопасности и киберпреступности на уровне ООН должен стать платформой для обеспечения мира, справедливости и безопасности в киберпространстве и должен содействовать разработке глобальной стратегии сдерживания угроз, возникающих с любой стороны. Процесс выработки Договора ООН о киберпространстве должен способствовать формированию общего понимания всех аспектов кибербезопасности во всех странах, находящихся на разных этапах экономического развития.

Все заинтересованные стороны должны прийти к общему пониманию того, что составляет киберпреступность, кибертерроризм и другие формы киберугроз. Это обязательное исходное условие для выработки национальных и международных решений, которые согласовывают меры кибербезопасности. Кроме того, общее понимание поможет также сократить разрыв между соответствующими оценками кибербезопасности в развитых и развивающихся странах. Учитывая что преступное поведение в киберпространстве имеет такой глобальный характер, необходимо глобальное согласование законодательства о киберпреступности, эффективная международная юстиция и сотрудничество полицейских сил, а также реальная воля осуществить все это.

---

[21] В 2009 году судья Шольберг и проф. С. Гернаути опубликовали первое предложение для выработки международного договора в форме небольшой публикации "Глобальный договор по кибербезопасности и киберпреступности – вклад в дело мира, справедливости и безопасности в киберпространстве", размещенной по адресу: (www.cybercrimedata.net). Эта работа была представлена на Форуме по вопросам управления использованием интернета в Шарм-эль-Шейхе: http://www.intgovforum.org/cms/2009-igf-sharm-el-sheikh. См. также публикацию Ахмада Камала, The Law of Cyber-Space. An Invitation to the Table of Negotiation. UNITAR, 2005. Посол Камаль в период написания этой работы был членом РМР, а ЮНИТАР является органом ООН.

Договор о киберпространстве на уровне ООН должен устанавливать принцип, согласно которому серьезные преступления против мира и безопасности, совершаемые через интернет и киберпространство, являются преступлениями по международному праву, независимо от того, наказуемы ли они по национальному праву. Мы твердо уверены в том, что наиболее серьезные преступления в киберпространстве следует определять и рассматривать по международному праву.

Заслуживает упоминания в связи с этим Конвенция Совета Европы о киберпреступности (2001 г.), которая, наконец, была введена в действие 1 июля 2004 года, и которая стала исторической вехой в борьбе с киберпреступностью[22]. Эта Конвенция представляет лишь один из примеров региональной инициативы, и многие страны предпочли использовать ее в качестве только справочного документа, так как она является и всегда будет европейским документом. Иными словами, необходимо создать на глобальной платформе на уровне ООН договор или свод договоров, включающий широко принятые стандартны и принципы этой Конвенции, но добавив определенные важные положения[23]. В действительности, как уже четко изложено в Глобальном стратегическом отчете МСЭ-HLEG, соответствующие меры связаны с правовыми, техническими и процедурными аспектами, в основе которых лежат организационные структуры, эффективные мощности и международное сотрудничество.

Соглашение о глобальном договоре стало бы дальнейшим шагом в развитие отчетов HLEG и шагом вперед в рамках инициативы МСЭ по ГПК, которая побуждает страны разрабатывать национальные программы кибербезопасности и осуществлять международное сотрудничество. Глобальный договор должен обязывать страны внедрять эту практику.

Концепция на будущее

Создание безопасного и надежного киберпространства потребует различных ресурсов и профессиональных знаний. Такой проект будет базироваться не только на специализированных технологиях и процедурах управления, особой нормативно-правовой базе, подлежащей применению на национальной основе и совместимой на международном уровне, но также на средствах управления и контроля, признанных и поддающихся проверке на международном уровне.

---

22 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

23 Ряд стран не принимают некоторые стандарты и принципы, в частности содержащийся в Статье 32 Конвенции принцип о трансграничном доступе к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным. Следует уважать точку зрения этих стран (Источник: Chairman's Report HLEG, ITU 2008).

Потребуется также определить некоторые основополагающие принципы, принять их и обеспечить их широкое признание международным сообществом, взяв за пример Всеобщую декларацию прав человека 1948 года[24].

Определить такие общепринятые ценности – непростая задача, учитывая различие стран, культур, а также экономических и политических интересов. Разработка глобального договора станет без сомнения долгим процессом. Именно поэтому необходимо срочно ввести механизм, содействующий международному диалогу, который будет завершен в сроки, соответствующие острой актуальности глобальных интересов.

Несмотря на сложности на пути создания такого договора и, безусловно, вероятность того, что он не всегда будет выполняться, грустной иллюстрацией чего служит приведенный мною пример Всеобщей декларации прав человека, этот договор тем не менее станет инструментом, используемым для борьбы с неправомерным поведением, независимо от того, допускают ли такое поведение отдельные люди, организации или государства. Наряду с этим такой договор должен помочь избежать отхода от общих ценностей или по крайней мере высвечивать расхождения, и в надлежащих случаях допускать компенсацию в соответствии с юридической практикой.

Вариант "договора о нераспространении кибертехнологий" может оказаться недостаточным, однако, поскольку он свел бы киберпространство и информационные технологии до статуса инструментов военного мира, которые могут использоваться как вооружения. Однако границы между военным и гражданским мирами нечеткие; используются те же технологии, и интернет один для всех – от самых молодых до самых пожилых пользователей.

Можно было бы провести аналогию с Договором о нераспространении ядерного оружия 1968 года[25], преимущества которого более не оспариваются, несмотря на постоянно возникающие сложности его применения; этот Договор не использовался в рамках предотвращения ядерного бедствия на Фукусиме в марте 2011 года, которое не было результатом военных действий. С другой стороны, организационная структура, такая как Международное агентство по атомной энергии (МАГАТЭ), продемонстрировала свою ценность в координации мониторинга этой катастрофы и выработке последующих мер безопасности. Применительно к киберпространству

---

24 http://www.un.org/en/documents/udhr/

25 Договор о нераспространении ядерного оружия. Был открыт для подписания в Лононе, Москве и Вашингтоне 1 июля 1968 года: http://www.un.org/en/disarmament/instruments/npt.shtml.

(УВРООН – Управление по вопросам разоружения: http://www.un.org/disarmament/;

ЮНИДИР – Институт Организации Объединенных Наций по исследованию проблем разоружения: http://www.unidir.org/html/en/home.html).

эквивалентная структура должна существовать, с тем чтобы содействовать безопасному, защищенному и мирному использованию информационно-коммуникационных технологий.

Эта заведомо смелая и ограниченная аналогия с ядерным оружием и атомными электростанциями не соответствует, безусловно, в полной мере необходимости в глобальном и всестороннем подходе к решению проблем безопасности киберпространства. Эти проблемы обусловливают принятие договора (или свода договоров), в котором признаются и военные и все прочие соответствующие аспекты.

Киберпространство несет выгоду преступникам всех видов, чья деятельность, такая как отмывание денег или торговля людьми, затрагивает военное и гражданское измерения. Но даже не учитывая эти конкретные соображения, допустимо ли, что в киберпространстве не соблюдаются права человека?

Интернет и киберпространство стали, на глобальном уровне, частью цивилизации, которую мы оставим в наследство будущим поколениям. Именно поэтому наша обязанность и ответственность – индивидуальная и коллективная – заключается в совместном определении общих ценностей, которые мы желали бы поддерживать и уважать на международном уровне, а также во внедрении механизмов надзора, обеспечивающих их уважение.

Меры по укреплению доверия

Каждый участник, создающий линию связи в цифровой цепочке, и каждая страна играют определенную роль, связанную с кибербезопасностью и кибердоверием. Безопасность имеет высокую цену, также как и цифровая незащищенность и отсутствие доверия. Сегодня расходы в связи с цифровой незащищенностью несут в основном пользователи и общество в целом, частично по линии полицейской и судебной систем, необходимых для борьбы с киберпреступностью, и частично в силу экономической нестабильности, вызываемой кибератаками, утечкой информации и кибершпионажем. Все эти действия могут привести, например, к несостоятельности предприятия, ущербу общественной репутации, утрате доверия клиентов, лишению доли рынка и потере рабочих мест.

Киберпространство не должно быть полем битвы или зоной организованной преступности, именно поэтому мы должны работать сообща и искать – честно и со всей искренностью – средства создания вызывающего доверие киберпространства для нашего и будущих поколений. Я уверена, что это будет достигнуто с помощью международного договора, действительной Всеобщей декларации прав всех людей (в том числе женщин и детей) в киберпространстве. Такой договор может внести вклад в укрепление доверия в киберпространстве, при условии готовности и приверженности на индивидуальном, организационном и государственном уровнях во всем мире соблюдать этот договор и разрабатывать учитывающую его практику.

Сознавая ограничения такого соглашения и тот факт, что это будет еще один международный договор, его основным преимуществом несомненно станет расширение осведомленности о необходимости обеспечения безопасности и доверия.

В совокупности мер по укреплению доверия такой договор – результат международного диалога – мог бы стать:

- реальным инструментом для повышения уровня осведомленности, для связи и для содействия решению вопросов безопасности и мира в киберпространстве и физическом мире;
- справочным документом, побуждающим участников экономической и институциональной сфер (в том числе полицейскую и судебную системы) внедрять передовой опыт;
- отправной точкой для разработки услуг и технологий, укрепляющих цифровое доверие и усиливающих судебные механизмы, и борьбы с киберпреступностью;
- инструментом, помогающим обеспечивать соблюдение минимального уровня безопасности в интернете, и снижающим уровень кибернасилия, с которым вынуждено мириться население.

Заключение

Настало время прагматичных действий, с тем чтобы сохранять и защищать наше цифровое наследие и содействовать его богатству, вносить вклад в развитие экономической безопасности, рабочих мест и конкурентоспособности. Это лишь некоторые из потребностей и задач для граждан, не говоря о необходимости настаивать на соблюдении их основных прав, которые в конечном счете для безопасности такие же, которые могут быть определены, при разной степени важности, для отдельных лиц, организаций и государств.

Вместе мы будем сильнее и сможем обеспечить согласованность и последовательность принимаемых мер безопасности. Более невозможно изолированно защищать цифровые территории, так как вирусы – биологические и электронные – не признают национальных границ. Не признают их и кибератаки, которые могут пронизывать многочисленные объекты инфраструктуры, в том числе принадлежащие нашим союзникам и соседям.

Защита инфраструктуры, развитие способности к восстановлению, борьба с киберпреступностью и усиление национальных позиций в области кибербезопасности и кибероборонны – это те действия, которые должны сегодня требоваться для хорошо информированного гражданина кибермира, для того чтобы создать прочное информационное общество.

Народная мудрость учит нас, что крыша, защищающая нас от дождя, была установлена в хорошую погоду: давайте же действовать, пока еще есть время.

Наивно и опасно было бы ожидать, что уязвимости исчезнут сами собой, и выявятся угрозы их использования. Мы должны предпринимать упреждающие действия и усиливать кибербезопасность, для того чтобы избежать, наряду с прочим, истребления наших информационных ресурсов, знаний, интеллектуальной собственности и личных данных, а также для того чтобы избежать непропорционального усиления и господства конкретных участников, независимо от того, являются ли они законными или преступными структурами.

Настало время, не проявляя наивности или острой паранойи, включить в наши стратегии безопасности тот факт, что интернет изменил способы проявления власти и создал новые формы конфликтов между отдельными лицами, между организациями и между государствами.

1.2 Подход ООН и Государств-Членов к нормам, правилам и принципам в области интернета: оценка доклада Группы правительственных экспертов ООН

Хеннинг Вегенер

Из результатов предыдущего анализа четко видно, что на международном уровне устойчивыми и даже экспоненциальными темпами растет осознание необходимости установления всеобщего порядка в киберпространстве и, в его рамках, норм ответственного поведения государственных субъектов и других заинтересованных сторон. Пусть даже киберсфера с момента своего появления и не была пространством, совершенно не подчиняющимся законам, правовым вакуумом, она несомненно продолжает оставаться местом, где отсутствует комплексная консенсуальная нормативно-правовая база, касающаяся не только государств, но и всех заинтересованных сторон. Постоянной задачей была и есть разработка в долгосрочной перспективе подходящей линии поведения, способствующей установлению универсальных норм. В рамках выполнения этой задачи, с учетом этого весьма универсального подхода, в настоящей статье акцентируется внимание на недавней деятельности ООН, более конкретно, на результатах работы специализированной Группы правительственных экспертов ООН.

За последние несколько лет произошел ряд событий в рамках прилагаемых в мировом масштабе усилий по нормативному регулированию киберпространства: серия резолюций ООН, принятых с 1998 года; принятие Будапештской конвенции по киберпреступности 2001 года; процесс ВВУИО; и развитие весьма важного национального законодательства в части гражданско-правовых режимов, регулирующих причинение вреда и нанесение ущерба, уголовного права,

административных актов, а также развитие соответствующего международного частного права. Однако все сходятся во мнении, что век систематической всесторонней кибердипломатии начался только примерно в 2008 году. С тех пор произошел всплеск международной активности; поражает изобилие инициатив и процессов, которые новым способом совместно приводят к складывающемуся консенсусу по вопросу о нормативных потребностях. Следует надеяться, что эти события, которые слишком многочисленны, чтобы их перечислить и проанализировать в одной работе[26], будут способствовать процессу, который носит "итеративный характер: каждый шаг основывается на уже достигнутых результатах"[27]. На многих из этих мероприятий используются полезные инструменты выработки мер по укреплению доверия или кодексов поведения, методы ведения переговоров, обсуждаемые в других частях данной публикации[28].

К счастью, на них уже подготовлен целый ряд очень хороших комплексных отчетов, которые содействуют осуществлению обзора и дальнейшей работе[29].

---

26 Вместо представления полного перечня ниже даются ссылки на наиболее актуальные из этих заседаний и их документы в соответствующем им контексте.

27 Документ A/68/98, стр. 11.

28 Мышление категориями кодексов поведения и мер по укреплению доверия или, как предпочитают некоторые, мер по укреплению прозрачности и доверия, очевидно, вытеснило более раннее увлечение концепцией всеохватывающей Конвенции по кибербезопасности, сравнимой с Конвенцией ООН по морскому праву 1982 года. Все чаще признавалось, что препятствия для создания такого документа носят непреодолимый характер. Возможно, киберпространство, является даже более сложным, чем мир океана. Цифровые технологии и виды их использования по-прежнему развиваются быстрыми темпами. Подготовку универсального договора преследовали бы еще большие расхождения во мнениях отдельных стран. Процесс переговоров о заключении договора занял бы много времени, а сроки осуществления национальных процедур ратификации даже близко не соответствовали бы неотложности задачи по заполнению правового вакуума и все более широко разделяемому пониманию того, что угроза киберконфликта и неуправляемого киберущерба выходит из-под контроля. Поэтому, хотя универсальные договор/право, регулирующие киберпространство, остаются предпочтительной целью, целевой концепцией, на данном этапе и, возможно, в обозримом будущем, альтернативный подход является более целесообразным по практическим соображениям.

29 Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas "**Baseline Review. ICT-Related Processes and International and** regional **Security** (2011−2013)" www.ict4peace.org, Geneva, March 2014; *Annegret Bendieck,* "Umstrittene Partnerschaft. Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit", DGAP, Berlin, December 2013. См. также *Henning Wegener,* "Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence-Building Measures", Erice, August 2012, размещено по адресу: www.unibw.de/infosecur.

Особенно плодотворным в части стимулирования этих мероприятий оказался двухгодичный период 2013–2014 годов. Помимо многих других результатов в этот период было создано как минимум три основополагающих документа: Таллиннское руководство о применимости международного права к киберконфликтам[30], документ NetMundial об управлении использованием интернета[31] и в особенности доклад Группы правительственных экспертов ООН, который был завершен летом 2013 года и представлен ГА ООН на ее 68-й сессии[32]. В этой публикации обсуждаются все три важнейших документа. В данной статье внимание сосредоточено на последнем докладе, а также при необходимости упоминаются другие документы и процессы.

Доклад 2013 года, подготовленный группой с непростым названием – Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности – не является отдельным результатом. Деятельность и мандат этой Группы, направленные на то, чтобы "[…] продолжить исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия в информационном пространстве, а также концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем", основаны на результатах работы предыдущей (2-й) ГПЭ и ее докладе, датированном июлем 2010 года (A/65/201). В докладе использованы общие направления, заданные серией поддержанных правительствами многосторонних конференций – от лондонской до будапештской, центральное место на которых заняло именно обсуждение норм и укрепления доверия, отраженных в мандате ГПЭ. Свой интеллектуальный вклад внесли многочисленные процессы консультаций в рамках региональных организаций и крупных международных органов, таких как ГА ООН, ЕС, Большая восьмерка, НАТО и региональные организации ООН. Поэтому в докладе ГПЭ отражены формирующиеся общие подходы и, в некоторых случаях, складывающийся консенсус. В нем представлена последовательность тщательно обдуманных соображений по имеющимся проблемам киберпространства. В тоже время доклад знаменует новый этап, в том смысле, что проблемы, которые уже обсуждаются в других местах, по-новому обобщены практически глобальной представительной группой правительств. Кроме того, продолжение процесса гарантировано благодаря созданию следующей (4-й) ГПЭ, имеющей еще более широкий, более представительный членский состав из 20 стран,

---

30 "Tallinn Manual on the International Law Applicable to Cyber Warfare" edited by Michael N. Schmitt. Подготовлено Международной группой экспертов по предложению Центра передового опыта по совместной защите от киберугроз при НАТО. Cambridge University Press 2013.

31 Многостороннее заявление NETmundial, http://netmundial.br.

32 Документ ООН A/68/98.

для дальнейшего изучения рекомендаций, содержащихся в докладе (A/RES/68/243), расширенный мандат которой предусматривает исследование "[…] вопросов использования информационно-коммуникационных технологий в конфликтах". Дополнительной гарантией являются новые международные мероприятия: в 2015 году Нидерланды примут у себя серию крупных конференций по киберпространству, в которых примут участие отдельные правительства в целях дальнейшего содействия складывающемуся консенсусу. Так, уже на Сеульской конференции по киберпространству, проведенной в октябре 2013 года вскоре после публикации доклада ГПЭ, собралось около 90 правительств, которые поддержали большинство рекомендаций этого доклада консенсусом, дословно процитировав его в своих Сеульских принципах и обязательствах в отношении открытого и безопасного киберпространства. И хотя доклад ГПЭ, как и многостороннее заявление NETmundial, не имеет обязательного характера, он придает многообещающий импульс будущим этапам достижения глобального консенсуса.

В данной статье главный интерес представляют две последние главы доклада ГПЭ, в которых содержатся рекомендации. Они включают рекомендации относительно норм, правил и принципов ответственного поведения государств и рекомендации по СВМ и обмену информацией. В связи с тем, что роль СВМ в обновленной концепции международной кибербезопасности является темой еще одной статьи для данной публикации, в последующих разделах будут рассмотрены основные выводы.

СВМ – напомним хотя бы их суть – способны уменьшить угрозы, повысить прозрачность, сделать поведение государств предсказуемым; они являются гибкими, добровольными и обеспечивают принцип переменной геометрии в отношении участников (возможно включение негосударственных субъектов) и последующих действий. В отличие от последовательного процесса заключения договора участники имеют право принимать частичные решения и вводить их в действие без задержки и самостоятельно или с другими заинтересованными сторонами, придерживающимися такого же мнения. СВМ, которые принимают государства, не требуют ратификации; они предлагают соревнование, и по большей мере – и в лучшем случае – имеют обязательную политическую силу. Таким образом, они идеально подходят для содействия процессу достижения международному консенсуса на эволюционной основе. Четко согласованный пакет СВМ при наличии критической массы участников может запустить процесс дальнейших последовательных изменений и рассмотрения более чувствительных вопросов. Уточнение стандартов поведения может обеспечить стимул для достижения большего.

Концепция СВМ была впервые опробована в условиях бывшего противостояния Восток-Запад в рамках прежнего СБСЕ и в ООН, а теперь она применяется повсеместно[33].

Рекомендации, содержащиеся в докладе ГПЭ, посвящены международному сотрудничеству, прозрачности, обмену срочной международной информацией, процедурам раннего предупреждения на круглосуточной ежедневной основе и механизмам CERT, согласованию правовых предписаний, правоохранительной деятельности, институциональному диалогу и другим "практическим" аспектам. Большим преимуществом является то, что в них также подчеркивается необходимость привлечения частного сектора и гражданского общества, содействуя таким образом принципам многостороннего участия. Они включены в перечни линий поведения, укрепляющего доверие, которые отчасти стали уже традиционными для других видов международной деятельности, и в них использованы такие комплекты рекомендательных мер, как Глобальная программа кибербезопасности МСЭ, в которой изложены задачи глобального сотрудничества, приводящего к созданию "[…] основы глобальной многосторонней стратегии международного сотрудничества" и диалога.

Во многих рекомендованных мерах также берется пример с мер, внедренных Большой восьмеркой в 1998 году, рамочного решения ЕС 2003 года и соответствующей главы Будапештской конвенции. Особую значимость имеет Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий[34], принятый недавно Постоянным советом ОБСЕ, так как членский состав этой организации охватывает широкий круг стран Востока и Запада, расположенных на большой географической территории, которые обычно демонстрируют разные мнения. В среде неправительственных организаций, безусловно, наиболее полный и систематизированный анализ СВМ в киберпространстве представлен в сборнике, составленном ICT4Peace, Женева, 2013 год, частично на базе Цюрихской конференции, созванной этой же великолепной организацией[35].

---

[33] В отношении более раннего этапа развития этой концепции в Европе и за ее пределами см. Henning Wegener "CBMs: European and Global Dimensions" in: F. Stephen Larrabee and Dietrich Stobbe, eds., "Confidence-Building Measures in Europe", Institute for East-West Studies, New York, 1983. Принятые ООН руководящие указания приводятся в документе ООН A/S-15/3. В отношении других применений см., например, Документ Монтрё о функционировании частных военных и охранных компаний в период вооруженного конфликта, www.icrc.org, или подготовленный ЕС проект Кодекса поведения в космической деятельности 2010 года, http://register.consilium.europa.eu.

[34] Документ ОБСЕ PC.DEC/1106 от 3 декабря 2013 года.

[35] "Confidence Building Measures and International Cyber Security", www.ict4peace.org.

Рекомендации, касающиеся норма, правил и принципов, возможно, более актуальны для обеспечения управляемого порядка в киберпространстве и кибербезопасности; поэтому они заслуживают более подробного рассмотрения. Также потребуется показать пробелы и неоднозначности в тексте, и, перейдя от первоначального анализа, отметить неосуществленные поручения и неотъемлемые задачи 4-й ГПЭ ООН на начальном этапе ее работы, а также другие основы кибербезопасности.

Значение краткого перечня важнейших норм и принципов обусловлено в значительной мере присоединением к консенсусу представителей правительств пяти постоянных членов Совета Безопасности ООН, а также Индии и Японии. Несмотря на его не имеющий обязательной силы характер, он, таким образом, является авторитетным справочным документом.

Во многих кругах подчеркивается, что особое значение имеет вывод Группы о том, что международное право, в особенности Устав ООН, в полной мере применимо к использованию ИКТ. Ранее данный принцип был выдвинут в нескольких международных документах, но никогда не был столь недвусмысленно сформулирован. Это является важным достижением, даже при том, что сразу же следует оговорка, сформулированная в двух других предложениях, где отмечается, что необходимо продолжать исследования вопроса о том, как эти нормы применяются к поведению государств, и что с учетом уникальных особенностей ИКТ в будущем могут быть разработаны дополнительные нормы.

Эти оговорки отражают известные устойчивые различия в подходах ряда крупных стран к глобальному управлению ИКТ, которые требовали компромисса на протяжении всего периода подготовки доклада. Поэтому сразу после пункта о применимости международного права следует пункт, подтверждающий распространение государственного суверенитета на деятельность, связанную с использованием ИКТ, а также на инфраструктуру, находящуюся под юрисдикцией государств.

Подтверждение действия международного права в киберпространстве включает, как указано в следующем пункте, уважение прав человека и основных свобод, закрепленных в соответствующих международных конвенциях. Этот принцип, пусть даже уже подчеркнутый во многих других международных документах, начиная с документов ВВУИО, безусловно имеет огромное значение для будущей свободы интернета и борьбы с правительственной цензурой в интернете.

Применимость Устава ООН также распространяет его основные положения на поддержание международного мира и безопасности, обязательство воздерживаться от угрозы силой и ее применения, а также право на самооборону в случае вооруженного нападения в рамках киберполя. Однако в преддверии продолжения исследования в докладе не рассматривается вопрос об использовании ИКТ во враждебных целях. Несмотря на то, что Группа была несомненно осведомлена о проекте Правил поведения в области обеспечения международной информационной

безопасности, представленных Россией, Китаем и другими странами в 2011 году,[36] – в главе Доклада по рекомендациям относительно норм содержатся явная ссылка на этот документ – она не включила текст, равноценный следующей норме из указанного выше проекта: "не использовать информационно-коммуникационные технологии, включая сети, для осуществления враждебных действий, актов агрессии, создания угроз международному миру и безопасности или распространения информационного оружия или соответствующих технологий", что по мнению автора данной статьи является досадным упущением. Вместе с тем остальные изложенные нормы и принципы, безусловно, достойны одобрения и представляются, в принципе, непротиворечивыми. В частности, это справедливо для рекомендаций о расширении сотрудничества против использования ИКТ в преступных или террористических целях, согласования правовых подходов и сотрудничества между правоохранительными органами и органами прокуратуры.

Не меньшего одобрения заслуживает список норм/принципов, изложенных в пункте 23 Доклада: государства должны выполнять свои международные обязательства в отношении приписываемых им международно противоправных деяний – вместе с тем трудно приписать злоупотребления в киберсреде; они не должны использовать посредников для совершения международно противоправных деяний; и должны стремиться не допускать того, чтобы их территория использовалась киберпреступниками – негосударственными субъектами. Юридически обязательное принятие этих норм и их перенос в национальное законодательство большим числом стран могло бы стать более эффективным инструментом противодействия деятельности операторов бот-сетей и киберпреступных синдикатов. Кроме того, следует надеяться, что оказание международного давления могло бы обеспечить применение необходимых правоохранительных мер на национальном уровне.

Наконец, текст включает нормативные ссылки на помощь частного сектора и гражданского общества в повышении кибербезопасности, включая более безопасное использование ИКТ, например "безопасность всей системы производства и сбыта информационных товаров и информационно-технических услуг". Это служит напоминанием о том, что обеспечение кибербезопасности является социально значимой задачей, требующей участия многих заинтересованных сторон и ответственности, которая должна выйти за рамки "ответственного поведения государств".

В совокупности различные разделы этого доклада – помимо части, касающейся норм/принципов, и главы, посвященной СВМ, есть также одна часть относительно мер по укреплению потенциала, содержащая полезные, хотя и менее впечатляющие рекомендации – представляют собой несомненный прогресс. Доклад не устраняет, но определенно уменьшает ряд важных принципиальных расхождений в позициях стран

---

[36] Документ A/66/359.

относительно будущего управления кибермиром. Устранение оставшихся различий по основным принципам является очень сложной задачей, особенно когда следующая ГПЭ будет "продолжать исследования" зарождающегося консенсуса и приступит к разработке подробных предписаний.

При этом доклад, подготовленный, фактически, по итогам работы серии крупных международных конференций (лондонской, будапештской, сеульской и др.) и региональных международных организаций, посвящен теперь двойному подходу, предусматривающему разработку СВМ и выработку норм и принципов для кодекса – или кодексов поведения в киберпространстве. Какие бы будущие форматы переговоров ни были приняты, данный подход сделает поведение государств более предсказуемым; он является гибким, добровольным и обеспечивает принцип переменной геометрии в отношении участников (государственных и негосударственных субъектов) и последующих действий: в отличие от последовательного процесса заключения договора, участники имеют право принимать частичные решения и вводить их в действие без задержки и самостоятельно или с другими заинтересованными сторонами, придерживающимися такого же мнения. Впрочем, ГПЭ достигла только частичного консенсуса, и проблемы, с которыми столкнется следующая ГПЭ, будут очень серьезными.

Группа была сформирована в конце июля 2014 года; в качестве председателя был избран ее член от Бразилии, и был согласован ее рабочий календарь, а также разделение труда между 20 правительственными экспертами. Теперь им предстоит подготовить или пересмотреть свои документы с изложением позиции и представить соответствующие проекты. Очередное собрание группы состоится в январе 2015 года с целью подготовки доклада к лету этого же года.

К первоочередным и наиболее сложным задачам ГПЭ относится подготовка более подробного определения международных правовых норм, относящихся к международной безопасности и миру, включая определение того, что является "вооруженным нападением" в терминах киберпространства; что представляет собой суверенитет в кибервек; каким образом можно сдержать использование кибертехнологий во враждебных целях ("кибероружие", включая вредоносное программное обеспечение, предназначенное для осуществления атак и нанесения ущерба военным и инфраструктурным объектам) и включить такое использование в нормативно-правовую базу. Эти вопросы преследуют нас с момента наступления кибервека, однако они стали более тревожащими в связи с безудержным наращиванием кибервооружений, осуществляемым все большим числом государств, которое стало частью нашей современной действительности, особенно в связи отсутствием в перспективе правовых и политических ограничений для этих зачастую необоснованных действий.

Таллиннское руководство, обсуждаемое в другой части данной публикации, несомненно, предлагает ценные идеи и руководящие указания для аналогий из

традиционного международного права, но, безусловно, является плодом работы преимущественно "западной" группы экспертов по правовым вопросам, который необходимо проверить на соответствие более глобальному видению. Критическая оценка этого руководства также показывает, что в анализе, в котором в качестве отправной точки используется, в основном, право вооруженных конфликтов, есть тенденция к признанию использования кибертехнологий во враждебных или военных целях как обычного варианта, по принципу "в жизни всякое бывает", хотя авторы руководства более или менее четко изложили ограничения и условия возможного использования. Вполне закономерно, что руководство, несмотря на его осторожные и тщательно подобранные формулировки, было истолковано во многих кругах как "приглашение к кибервойне". Безусловно, было бы уместно сделать важные оговорки, в которых подчеркивается основное положение о недопустимости кибервойны и присущие ей опасности.

Дополнительная проблема неизбежно связана с общим характером рекомендаций, содержащихся в докладе. В каждом случае их преобразование в практические меры и детальное наполнение общих предписаний будет чрезвычайно сложно осуществить, тем более что необходимо регулировать участие различных региональных процессов и широкого многостороннего сообщества, с тем чтобы добиться непротиворечивых итоговых документов.

При таких обстоятельствах создание форума – или форумов – на которых могут начаться интенсивные обсуждения и последующие переговоры, является весьма сложной задачей. В докладе ГПЭ рекомендуется поддерживать регулярный институциональный диалог с широким кругом участников под эгидой ООН, а также регулярный диалог в рамках двусторонних, региональных и многосторонних форумов и других международных организаций. Это, безусловно, шаг в правильном направлении, однако слишком неконкретный, чтобы обеспечить возможность быстрого принятия решения по дальнейшим процедурным шагам. Вероятно, было бы целесообразно сузить институциональный выбор за счет согласования в первую очередь критериев проведения форума (открытый и всеобъемлющий характер, обеспечивающий полноправное участие более широкого сообщества заинтересованных сторон, поддержка опытного международного секретариата, обладающего квалифицированными кадрами в области ИКТ и т. д.). Конечно, наиболее желательным направлением было бы создание единого форума, предлагающего универсальный подход. С другой стороны, уже осуществляется предварительная региональная деятельность, и следует использовать ее динамику. Приемлемой площадкой, вероятно, могла бы считаться самостоятельная конференция государств, на которой могут быть установлены собственные правила процедуры и условия широкого участия заинтересованных сторон.

Возвращаясь к главе доклада, в которой приводятся рекомендации в отношении норм, правил и принципов, следует напомнить, при всем уважении к работе авторов, что их перечень, с учетом политических особенностей контекста ООН и необходимости

достижения консенсуса в сжатые сроки, является выборочным и далеко не полным. Безусловно, следующая 4-я ГПЭ должна внимательно изучить дополнительные нормы и принципы, представленные в последнее время[37].

В частности, необходимо в более явной форме установить нормы в основных областях безопасности, киберстабильности и кибермира[38]. Представляется, что следует заполнить, например, следующие пробелы: призыв к имеющему обязательную силу договору об основном принципе, что кибератака другого государства, осуществляемая непосредственно или с использованием наемных исполнителей, является нарушением международного права; обязательство всех государств первыми не прибегать к использованию кибероружия против другого государства, при условии что оно не подверглось нападению с использованием обычных видов вооружения. Государствам следует также придерживаться на национальном и международном уровнях политики предотвращения киберконфликтов, придавая значение киберзащите, ограничению и лишению легитимности разработки, использования и экспорта наступательных киберсредств, в особенности специализированного программного обеспечения для осуществления атак. Следует защищать важнейшие инфраструктуры сверх того, что предлагается в пункте 26 (e), и расширять международное сотрудничество, руководствуясь принципом, что Государства несут ответственность за защиту важнейших инфраструктур на своей национальной территории, что что атаки на эти инфраструктуры запрещены, гарантируя тем самым неприкосновенность структур транснациональных цифровых сетей. Кроме того, все еще отсутствует принцип, согласно которому государства обязаны защищать своих граждан в киберпространстве. Выходя за рамки рекомендации, содержащейся в пункте 23, следует указать, что запрещено использовать бот-сети и осуществлять другие незаконные киберпреступные/боевые действия, и что государства обязаны ввести данный запрет на своей национальной территории. Наконец, принцип нейтралитета продолжает действовать и в кибервек, и кибератаки, даже в целях самообороны, не должны совершаться с использованием сетевых структур нейтральных государств.

---

37 Помимо работы региональных организаций, частично перечисленных в пункте 27 доклада ГПЭ, см. упомянутые ранее работу ICT4Peace, прим. 6, выше; статью Хеннинга Вегенера, прим. 3, выше, пять принципов кибермира, изложенных Генеральным секретарем МСЭ, которые приведены в Декларации Эриче о принципах киберстабильности и кибермира 2009 года, приведенной в публикации "В поисках кибермира", стр. 110.

38 В мандате вновь образованной 4-й ГПЭ делается акцент на сценариях "конфликтов".

1.3 Применяется ли международное прав к киберпространству?

Габор Иклоди

Цифровой век обеспечивает огромные преимущества, но также несет многочисленные угрозы, способные вызвать масштабные нарушения и даже разрушения. Перед нами стоит принципиальная задача поиска способов защиты киберпространства как доверенной среды, по которой мы можем свободно перемещаться и в полной мере использовать ее потенциал, но делать это более "бдительным" образом. Для этого требуется найти надлежащий баланс между свободой и безопасностью, и здесь не подходит ни игнорирование рисков безопасности, ни их использование в качестве предлога для ограничения свободы и гражданских свобод. Для того, чтобы преобладало доверие, важно обеспечить, чтобы правительственные учреждения в полной мере соблюдали требования демократический подотчетности, стремясь предотвратить вредоносную деятельность в киберпространстве.

Доверие имеет принципиальное значение для граждан и в не меньшей степени для государств в их международных отношениях, которым посвящена данная статья. Сегодня мы стали свидетелями своего рода холодной кибервойны, ведущейся в условиях повышенного уровня кибершпионажа и больших инвестиций в наступательные кибервозможности, в основном, со стороны развитых стран, быстро адаптирующихся к изменениям.

С точки зрения любого современного военного, важно не допустить снижения его возможности беспрепятственного осуществления маневра в киберпространстве. Данное требование четко отражено во все большем количестве национальных оборонных стратегий, признающих киберпространство в качестве "новой сферы ведения боевых действий, которая так же важна для военных операций, как и суша, море и космос"[39]. Вывод совершенно очевиден: киберпространство стало частью современной войны, и вероятно, масштабные конфликты будут протекать только при наличии существенной киберсоставляющей. Опыт прошлых лет служит тому достаточным доказательством.

Для того чтобы киберпространство стало и оставалось сферой доверительных отношений, предлагается создать атмосферу сотрудничества, в которой применяются определенные общепринятые правила. Важными составляющими этой атмосферы являются международные нормы, регулирующие поведение государств. Однако следует подчеркнуть, что, несмотря на их очевидную актуальность, они являются не единственными составляющими. Киберпространство – это единая сфера, имеющая многосторонний характер, в которой правительства отнюдь не единственные

---

[39] Политика НАТО в области киберзащиты, Брюссель, 8 июня 2010 г.

участники, формирующие эту атмосферу. Необходимость разработки и поддержания истинного партнерства государственного и частного секторов в киберпространстве выше, чем в любой другой сфере. "Именно частный сектор владеет большей частью киберинфраструктуры и эксплуатирует ее, и именно этот сектор создает нужные всем нам технологии. Частный сектор представляет собой первую линию обороны, при этом частные компании и наука проектируют будущую технологическую среду, в которой будут работать и правительства"[40] Это, конечно, не уменьшает преимущественные обязанности правительств, вытекающие из того, что влечет за собой суверенитет, и от исполнения которых они не могут уклониться.

Сегодня не существует договорных положений и обычных норм, предназначенных конкретно для киберпространства. Но означает ли это, что киберпространство должно считаться совершенно нерегулируемой сферой, своего рода "Диким Западом", где совсем не действуют какие бы то ни было нормы? Действительно ли обосновано утверждение, что должен быть в срочном порядке выработан комплекс норм, имеющий обязательную силу, и осуществимо ли это на практике? Или же отправная позиция должна быть скорее такой, как ее изложил Министр иностранных дел Соединенного Королевства Уильям Хейг: "Поведение, которое неприемлемо в офлайновой среде, также неприемлемо в онлайновой среде, будь то поведение частных лиц или правительств"[41].

Применимость международного права в киберпространстве

В течение довольно длительного времени среди экспертов ведется дискуссия о том, применимы ли международные документы, разработанные для традиционных сфер, и к киберпространству. Дебаты несколько сбавили обороты после террористического акта, совершенного 11 сентября 2001 года, когда акцент сместился на борьбу с терроризмом, однако вновь оживились примерно в период 2007–2008 годов. Внимание к терроризму придало много актуальных аспектов этим оживившимся дебатам о киберпространстве, поставив следующие вопросы: как приписать действие негосударственных субъектов тому или иному государству; каковы обязанности одного государства в отношении деятельности таких групп, действующих на его территории и осуществляющих нападения на объекты в другом государстве; каким образом на законном основании использовать силу против негосударственных субъектов, находящихся в другом государстве; и можно ли использовать силу для нанесения упреждающего удара в преддверии нападения, чреватого тяжкими

---

40 Габор Иклоди: Выступление на Симпозиуме НАТО по обеспечению целостности и безопасности информации, 11 сентября 2012 г., Монс.

41 Выступление Министра иностранных дел Соединенного Королевства Уильяма Хейга 11 ноября 2011 года на первой Конференции по киберпространству в Лондоне.

последствиями, и если можно, то при каких условиях? Все эти вопросы чрезвычайно актуальны и в киберсреде.

Идея о том, чтобы выработать глобальное соглашение, имеющее обязательную юридическую силу, которое устанавливало бы большинство норм, подлежащих соблюдению в киберпространстве, и описывало бы последствия их несоблюдения, может показаться заманчивой. Однако в настоящее время, она, по-видимому, выходит за рамки возможного и, более того, даже необходимого, и тому есть множество причин. Во-первых, эта сфера развивается столь быстрыми темпами, что было бы практически невозможно согласовать всеобъемлющий и устойчивый комплекс норм, относящихся к киберпространству. Во-вторых, очевидно, что страны существенно расходятся во мнениях по целому ряду важнейших вопросов, имеющих практические последствия, таких как пороговые уровни, реагирование и правоохранительная деятельность. Поэтому, пытаясь сегодня окончательно зафиксировать наше представление о киберпространстве и, что не менее важно, то, о чем можно было бы договориться, мы связали бы себя ограничениями, что в действительности может оказаться неэффективным (в частности, в странах, более приверженных строгому соблюдению законов). В-третьих, ценность правовых обязательств, выполнение которых практически невозможно проконтролировать, весьма сомнительна.

Как показал опыт, полученный в других областях, включая контроль над вооружениями и ядерное разоружение, при повышенном уровне недоверия между сторонами достижению результатов в большей более способствует выбор тактики маленьких шагов, которые на первом этапе могут постепенно укрепить и упрочить доверие, шаг за шагом, а не установление высокой планки и попытка преодолеть очевидные трудности. В этом отношении ряд очень важных уроков был извлечен из опыта, полученного в области контроля над ядерным вооружением. Достижению этой цели могут способствовать меры, которые оставляют открытыми каналы взаимодействия, обеспечивают определенную степень прозрачности и помогают разрядить напряженную обстановку во время кризиса. Двусторонние и региональные инициативы, например работа ОБСЕ в области кибердоверия и мер по укреплению безопасности, указывают правильное направление, но, кроме того, отражают, насколько сложно прийти к согласию, даже если предложенные меры затрагивают второстепенные вопросы и имеют добровольный характер.

Это не значит, что было бы преждевременно изучать сейчас вопрос о международных переговорах и сотрудничестве. Наряду с СВМ, содействующими созданию необходимой среды для более строгих мер, есть области, в которых было бы относительно легко начать работу. Как полагает Джо Най, "наиболее перспективными областями международного сотрудничества являются не двусторонние конфликты, а проблемы, создаваемые третьими сторонами, например преступниками и

террористами"[42]. По всей вероятности, интересы развитых (и поэтому более уязвимых) государств в ограничении ущерба, причиненного преступными и террористическими группами, в долгосрочной перспективе будут совпадать, что в свою очередь откроет им возможности для сотрудничества в области криминалистики и средств контроля. "Государства могут для начала взять на себя ответственность за атаки, осуществляемые с использованием их территории, и обязанность сотрудничать в области криминалистики, обмена информацией и мер по устранению последствий"[43].

Что касается международных норм, то дальнейшие шаги, очевидно, заключаются в принятии за основу соответствующих существующих правовых документов, как в части *права войны* (право, регулирующее применение силы), так и *законов военного времени* (право, регулирующее протекание вооруженного конфликта), а также их применении к киберпространству. Такое общее согласие позволило бы нам тогда продвинуться дальше и последовательно оценить, какие положения существующих правовых документов требуют общего толкования, а какие необходимо дополнить.

За прошедшие почти два года были предприняты две важные международные попытки обеспечить общее понимание в отношении основных аспектов этой проблемы, т. е. кибератак. И в Таллиннском руководстве, подготовленном группой независимых ученых и практикующих специалистов в области международного права под эгидой Центра передового опыта по совместной защите от киберугроз (CCD COE) при НАТО, и в рекомендациях, подготовленных Группой правительственных экспертов ООН (ГПЭ ООН) в области ИТ подтверждено, что существующее международное право, безусловно, применяется и к киберпространству.

Следовательно, вопрос заключается не в том, применяются ли существующие законы, а скорее в том, каким образом они применяются. Следует признать, что выводы обеих групп не имеют обязательной силы и не были согласованы государствами – по крайней мере пока. Тем не менее достигнутое среди экспертов согласие справедливо названо знаковым консенсусом.

Таллиннское руководство[44] является довольно проработанным и серьезным академическим исследованием, которое подготовлено по предложению расположенного в Таллинне Центра передового опыта по совместной защите от киберугроз (CCDCOE) при НАТО. В нем всесторонне рассматривается вопрос о том, в какой степени правовые нормы могут применяться в случае кибервойны. В нем отражены мнения тех независимых экспертов, которые участвовали в работе Группы, и не более того. Правильнее всего рассматривать его как предпринятую Группой

---

42 Joseph S. Nye: "Nuclear Lessons for Cyber Security" in *Strategic Studies Quarterly*, Winter, 2011.

43 Eneken Tikk: "Ten Rules of Security", *Survival*, June-July 2011.

44 Таллиннское руководство по международному праву, применимому в случае кибервойны.

искреннюю попытку запустить мыслительный процесс, касающийся комплекса весьма деликатных и важных вопросов. Другими словами, это приглашение другим сторонам принять участие в мыслительном процессе, а также скорее начало, чем конец попыток добиться разделяемого всеми общего понимания.

Что составляет понятия "применение силы" или "вооруженное нападение" в киберпространстве?

Мы очень хорошо понимаем, что такое военные действия, но какой юридический смысл имеют термины "применение силы" и "вооруженное нападение" в киберизмерении? Может ли некинетическое действие, каковым является кибератака, быть "вооруженным нападением", или это так только в случае, если оно составляет часть более широкой кинетической операции? Какой вид реагирования на кибератаку может считаться законным, и включает ли оно право на применение в ответ военной силы?

Термин "кибервойна" не имеет общепринятого согласованного определения. Термин используется, как правило, для описания враждебных действий в киберпространстве "[…], результаты которых дополняют или эквивалентны применению грубой кинетической силы"[45]. Таким образом, это не просто развертывание средств нападения, но скорее последствия их применения, которые могут помочь нам определить, ведется ли кибервойна. На текущий момент никто не видел кибервойны в строгом смысле этого слова. Мы были свидетелями массовых атак типа "отказ в обслуживании", направленных на ту или иную страну или ее важнейшую инфраструктуру, как отдельной атаки или части более крупного кинетического наступления, и мы видели целевые атаки против промышленных систем управления. "Однако проблемы непредвиденных последствий и каскадных эффектов не возникали, […и поэтому] полный комплекс мер и ответных действий в кибервойне между государствами не исследовался"[46].

В Уставе Организации Объединенных Наций предусмотрены лишь два исключения из общего запрета применения силы: одно в Главе VII, где в случае если Совет Безопасности определяет существование любой угрозы миру, он уполномочивается предпринимать такие действия, которые он сочтет необходимыми для восстановления мира; и другое – в Статье 51, когда страна осуществляет свое право на самооборону, которым со всей очевидностью признается ее неотъемлемое право на применение силы против агрессора в индивидуальном или коллективном порядке.

Здесь уместно привести ряд общих наблюдений. Как показывает практика, получить разрешение Совета Безопасности ООН на применение силы весьма сложно. Это

---

45 Joseph S. Nye, там же.

46 Там же.

обусловлено в основном требованием единогласия "великих держав" или, иными словами, правом "вето", которым обладают постоянные члены Совета Безопасности. Достичь единогласия подчас трудно, особенно в случаях, когда один или несколько постоянных членов являются сторонами рассматриваемого конфликта. Это, не говоря о противоречии демократическому характеру процесса, косвенно несет в себе риск того, что страны отдадут предпочтение классификации случая применения силы как вооруженного нападения, что соответственно даст им основания для применения силы против агрессора. Еще одним фактором, усиливающим сдвиг в сторону расширенного применения Статьи 51, является складывающееся применение права государств на самооборону в случае террористических атак.

Что происходит, когда нападающим является или оказывается не государство, а негосударственный субъект? Создатели Устава ООН намеренно оставили понятие "вооруженное нападение" открытым для интерпретации ее органами и государствами-членами. Кроме того, в Статье 51 использована достаточно широкая формулировка, для того чтобы предоставить подвергшимся нападению государствам возможность самообороны, даже если инициатором нападения являются негосударственные субъекты. Реакция на атаки, предпринятые 11 сентября, служит важным примером как касающимся процесса принятия решений Советом Безопасности ООН, так и оперативных решений НАТО.

Однако могут ли некинетические кибероперации составить "применение силы" и даже "вооруженное нападение", или, следуя логике создателей Устава ООН, эти термины применяются только к использованию военной силы? За прошедшие годы предпринимались многочисленные попытки разъяснить, может ли политическое и экономическое принуждение приравниваться к применению силы. Эти попытки в большинстве своем потерпели неудачу, так как многие опасались, что признать некинетические несиловые действия как возможные причины ответного применения силы означало бы просто открыть ящик Пандоры. Однако действительно ли правильно сосредотачиваться исключительно на используемых инструментах, или, напротив, следует уделять больше внимания и придавать большее значение вызываемым ими последствиям?

Для правительств исторически вероятно менее значимо то, какие конкретные инструменты использовались в ходе данного события, по сравнению с тем, каковы были последствия их использования. Вспомним атаки 11 сентября, когда гражданские воздушные суда использовались с намерением нанести максимальный возможный ущерб и убить людей. Итак, можно принять следующее правило: если кибератаки ведут к разрушительным последствиям, сравнимым с последствиями кинетического воздействия, то кибератаки следует рассматривать как применение силы и даже как вооруженное нападение, аналогичное военному наступлению. В таком аспекте не имеет значения, предпринято ли нападение с воздуха, суши, моря или из киберпространства; именно последствия атаки все в большей степени будут определять, как трактовать нападение, и обусловливать право страны, на которую

совершено нападение, принимать меры самообороны. Другим примером может служить Сирия. Выброс химических веществ смертельного действия в целом классифицируется как некинетическое действие. Однако их использование в Сирии против местного населения, которое вызвало массовую гибель и поражение людей, может, вероятно, трактоваться как применение силы.

Более сложным случаем представляется происшествие с нефтяной компанией Saudi Aramco в 2012 году. Несмотря на то, что полное уничтожение всех данных, хранившихся на более чем 30 000 компьютерах компании, несомненно стало чрезвычайно болезненным ударом и создало ситуацию, которая сделала сложным и дорогостоящим даже частичную ликвидацию последствий, многие эксперты предостерегали от определения этой ситуации как вооруженного нападения со всеми вытекающими последствиями.

Как же определить, попадает ли событие в рамки определения "применение силы", потенциально также составляя "вооруженное нападение"? Насколько сильным должен быть ущерб, боль или страх, для того чтобы сделать заключение о необходимости начала ответных действий?

К сожалению, однозначного ответа на этот вопрос не существует. Однако общее соображение, приведенное выше, остается справедливым. А именно, если последствия атаки столь же серьезны, как и последствия традиционного нападения, такая атака может рассматриваться как применением силы[47]. Существует, следовательно, очевидная связь с тяжестью ущерба и числом жертв, которые стали результатом нападения. События, повлекшие за собой многочисленные жертвы, определенно попадают в эту категорию, также как вероятно и атаки, парализующие ключевые сферы жизни в стране. Однако возможно ли установить порог для такого определения? Ответ – безусловно, невозможно. Решение о том, чтобы характеризовать событие как "применение силы" или "вооруженное нападение" всегда будет приниматься для данного конкретного случая и базироваться на многочисленных различных факторах. В таком аспекте заключение о том, что составляет военные действия, в большей степени вопрос политической, а не военной или правовой оценки. Конкретное определение невозможно. Даже в случае террористического акта, после ужаса 11 сентября точность невозможна. Можем ли мы, например, заключить, что если целью террористической атаки является невинное гражданское население и общее число погибших превышает 3000, то это однозначно военное нападение? Хотели бы мы, таким образом, обозначить, что если численность жертв не превышает порога в 3000, то нападение не должно рассматриваться как вооруженное нападение? Не говоря о любых иных соображениях, не является ли это

---

47 См. так называемый "критерий Шмитта", представляющий собой свод правил, которые могут помочь государству решить, является или не является кибератака военными действиями.

неким сообщением, предназначенным для потенциальных исполнителей преступлений? Я уверен в отсутствии такого намерения.

Кибероперации могут классифицироваться самыми разными способами. Одной из общепринятых моделей является триада "конфиденциальность, целостность и доступность" (КЦД), сформулированная для определенная проблемных областей и решений в сфере информационных технологий[48]. Атаки, направленные на целостность, которые специально разработаны для срыва нормального функционирования систем управления (как например, вирус Stuxnet), или атаки, направленные на доступность (блокирование управления воздушным движением, как в Грузии), могут привести к жертвам, и их последствия могут быть сравнимы с последствиями кинетических атак. Следовательно, они могут относительно легко преодолеть порог определения применения силы. С другой стороны, атаки на конфиденциальность (шпионаж с помощью киберсредств) может привести к огромным потерям (только в США кража интеллектуальной собственности оценивается примерно в 250 млрд. долл. США в год), но эти атаки попадают в другую категорию, и в ответ на них предпринимаются в основном дипломатические действия.

Шпионаж, будучи второй древнейшей профессией, практикуется весьма широко, иногда даже среди ближайших союзников. "На макроуровне каждое государство должно уравновешивать зачастую противоречащие цели обеспечения максимальной свободы действий и минимального вреда. При отслеживании злонамеренного поведения преследуется цель минимизации вреда, то есть выявление угрозы на достаточно раннем этапе, чтобы не позволить причинение вреда"[49]. В эпоху, когда предупреждение и ранее обнаружение враждебного намерения и вредоносного действия приобретают все большую важность, для того чтобы предотвращать инциденты, а не пытаться бороться с их последствиями, возрастает значение разведки. Объявление киберразведки полностью вне закона в международных отношениях трудно назвать реалистической задачей. Однако "[…] вполне возможно представить процесс итераций (око за око), ведущий к разработке правил игры, которые позволят ограничить ущерб в практическом аспекте"[50].

В то же время интерес к снижению планки применения силы как средства сдерживания экспансии шпионажа весьма заметен в идеях ряда стран, в особенности менее развитых стран. В более развитых странах наблюдается более колоритная картина. Эти страны весьма часто становятся основными целями таких шпионских атак, а с ругой стороны, эти страны в наибольшей степени заинтересованы в сохранении широкой возможности для маневра и, таким образом, в целом не поддерживают идеи

---

48 См. Darril Gibson "Understanding The Security Triad", *Pearson*, 27 May 2011.

49 Интервью с Ка-Кин Хо, руководителем по вопросам кибербезопасности компании CISCO.

50 Joseph S. Nye, там же.

снижения планки. Как страны, желающие иметь бóльшую свободу действий при применении ответных мер и обладающие необходимыми для этого возможностями, они также более заинтересованы, в целом в сокращении разрыва между порогом для "применения силы" и "вооруженного нападения".

Реагирование на кибератаки

Для страны, подвергшейся массированной кибератаке, самая важная первоочередная задача заключается в том, чтобы остановить и отразить атаку и в кратчайшие сроки восстановить поврежденные системы. Таким образом, приоритетами являются защита населения и восстановление важнейших цифровых сетей. В большинстве случаев цель заключается в том, чтобы не допустить дальнейшей эскалации конфликта, если только для отражения и предупреждения будущих атак не рассматривается необходимым применение силы.

Крупная кибератака, содержащая, например, вредоносный код, который выводит из строя управление воздушным движением, и вызывающая столкновение или падение на землю самолетов и многочисленные жертвы, вероятно будет рассматриваться как вооруженное нападение, требующее адекватного реагирования. Но даже и в таком случае в соответствии с международным гуманитарным правом реагирование должно отвечать определенным важным критериям. Оно должно быть пропорциональным, обоснованным и необходимым и должно базироваться на принципах различия и возможных предупредительных мер в отношении атак. Что касается содержания, реагирование может иметь различные формы. Оно может быть военным или кибернетическим, или же это может быть объявление и изобличение злоумышленника в рамках ООН, либо это может быть дипломатический ответ или введение санкций. И опять-таки ответные меры могут вовсе не приниматься.

Учения, воспроизводящие реальные сценарии, со всей очевидностью продемонстрировали, что массовые направленные кибератаки, предпринимаемые эффективным и продуктивным злоумышленником, который намерен нанести серьезный ущерб, не могут быть остановлены с помощью только киберсредств. Это еще более очевидно, если кибератаки составляют часть более крупной наступательной кампании. Оборонительные кибермеры могут помочь в восстановлении поврежденных сетей, содействовать проведению экспертизы и раннему обнаружению, но они не могут избавить от угрозы. Для этого требуется принятие иных мер в рамках национального арсенала средств.

Упреждающие действия

Еще один интересный аспект этой проблемы связан с особенностями киберизмерения, то есть с тем, что факторы времени и пространства в значительной степени утрачивают свою актуальность: времени для предупреждения почти нет или вообще нет. Время между обнаружением компьютером вероятности нападения на

него агрессивного вредоносного кода и упреждающим шагом для обезвреживания атаки может составлять всего несколько миллисекунд. Эффективная защита, таким образом, предполагает автоматические ответные меры, которые сами по себе обусловливают ряд сложных вопросов. Учитывая скорость атаки, вопрос заключается в том, должно ли государство ожидать, когда произойдет массированная кибератака, аналогичная вооруженному нападению (как самостоятельное действие, направленное на важнейшую инфраструктуру этого государства или как часть кинетической операции, направленной на вывод из строя жизненно важных командных и контрольных центров), или ему следует разрешить осуществлять упреждающее ответное действие. Если это так, то в какой момент должно вмешиваться государство в целях предотвращения разрушительных кибератак – каковы условия упреждающей самообороны?

Многие профессиональные юристы приняли, как представляется, стандарт, известный как "последнее имеющееся окно возможностей", когда бездействие в этот момент создает риск серьезного нарушения эффективной обороны. В Таллиннском руководстве делается заключение о том, что государство может действовать в порядке самообороны "[…] если нападающий очевидно намерен осуществить вооруженное нападение, а государство-жертва в случае бездействия утратит возможность эффективно защищать себя"[51].

Применение киберсредств рассматривается зачастую как альтернатива чему-то худшему. Передовые и могущественные страны могут почувствовать искушение перейти к более широкому стратегическому использованию кибероружия, для того чтобы убедить противника изменить свое поведение или прекратить определенные опасные действия. Это может быть хорошо, если предотвратит войну. В то же время это может привести к тому, что прочие страны почувствуют себя уязвимыми, беззащитными перед другими, более передовыми участниками. Страх, что это может развязать еще более широкую гонку кибервооружений, когда страны будут пытаться захватить или привлечь кибернаемников, вовсе не лишен основания. Беспокойство вызывает также то, что код часто предпринимаемых сложных кибератак становится доступным через интернет негосударственным субъектам.

Каков уровень доказательств, необходимых для отнесения?

Отнесение кибератаки к конкретному исполнителю с достаточной степенью уверенности приводится зачастую в качестве одной из основных проблем – той, которая фактически делает определение кибероперации как "вооруженного нападения" практически невозможным. Несомненно, это реальная проблема и было бы ошибкой игнорировать ее. Но не следует при этом и придавать ей слишком большое значение. Международные условия, способствующие упрочению

---

[51] Таллиннское руководство по международному праву, применимому в случае кибервойны.

сотрудничества, более тесное взаимодействие разведывательного и кибертехнического сообществ и не в последнюю очередь развитие технологий – все это может способствовать улучшению ситуации.

Если действительно требование заключается в представлении очевидных и убедительных доказательств связи атаки с исполнителем таким образом, чтобы их можно было представить в суде, тогда проблема отнесения действительно весьма сложная. Но отнесение – понятие относительное. Следует признать тот факт, что в случае кибератаки найти "дымящийся пистолет" практически невозможно. Полная, абсолютная достоверность может быть установлена в редких случаях, даже спустя недели после атаки, если вообще может быть установлена. Использование в качестве основы растущего количества улик, собираемых в различных областях (разведка, техническая область и. т. д.) является более реалистичной перспективой (т. е. существование "косвенных доказательств"). Отнесение является относительным понятием и в реальной политике. Опасения, связанные с трудностями отнесения атаки к тому или иному исполнителю соразмерны числу жертв. Другими словами, чем выше число погибших, тем сильнее давление на правительства с требованием решительного реагирования на атаку.

Важно также подчеркнуть, что отнесение не является требованием, для того чтобы квалифицировать атаку как военное нападение. Вспомним реакцию НАТО на события 11 сентября, когда в течение 24 часов Альянс привел в действие, впервые в своей истории, механизм коллективной самообороны, предусмотренный Статьей 5. В использовавшейся далее НАТО формулировке не упоминалась относимость террористической атаки к государству. Был просто поставлен вопрос о том, была ли атака против США направлена из-за рубежа, – требование, цель которого убедиться, что положение о коллективной обороне не используется против собственных граждан. Часто делается заключение о том, что устрашение не действует в киберпространстве в силу проблемы отнесения. Без сомнения, это отчасти верно, хотя и не в традиционном смысле, когда достаточно продемонстрировать силу, для того чтобы остановить потенциального агрессора. Однако устрашение действует в ситуациях, когда оно может лишить выгод атаки, а не в случае попытки навязать расходы, связанные с ответными действиями, аналогично тому, как противоракетная оборона делает атаку неэффективной или чрезмерно дорогостоящей. "Атаки становятся менее привлекательными, если сильны брандмауэры или вероятна перспектива автоматического реагирования"[52].

Негосударственные субъекты

В киберпространстве, согласно большинству оценок на основе разведданных, лишь ограниченное число государств обладают в настоящее время возможностью

---

[52] Joseph S. Nye, там же.

осуществлять сложные и устойчивые атаки, наносящие серьезный ущерб. В то же время, как заявил заместитель министра обороны Линн, "[…] при том что государства обладают наибольшими возможностями, атаку с катастрофическими последствиями скорее всего предпримут негосударственные субъекты"[53].

Здесь я хотел бы остановиться и провести четкое различие между шпионажем, с одной стороны, и сокрушительным нарушением и разрушением, с другой стороны, даже если в техническом смысле эти понятия весьма близки. При том что безусловно следует делать все возможное, для того чтобы затруднить шпионаж и кражу ценной государственной и промышленной информации, устранение риска атак, вызывающих массовое уничтожение, является неоспоримым приоритетом.

Хорошую новость составляет тот факт, что в области ядерных стратегий государства используют, как правило, разумные доводы и скорее всего будут воздерживаться от пересечения критической черты, за которым последует жесткая реакция. Для того чтобы страны поняли эту ситуацию, им следует прежде всего знать, что критическая черта действительно проведена. Поэтому сигнал должен быть громким и четким: разрушительная атака может вызвать принятие национальных или коллективных контрмер, когда возможно применение любых средств из арсенала[54]. Во-вторых, существует возможность постепенной разработки определенных мер по укреплению доверия, мер по снижению эскалации и некоторых базовых правил, о которых говорилось выше, и опять на основе опыта, полученного в ядерной области.

Сложнее ожидать рационального мышления от некоторых "государств-изгоев", которые стремятся создать наступательный киберпотенциал и инвестируют в это направление значительные средства. Их сложнее сдерживать и, о чем напоминают нам аналитики в ряде нестабильных районов, для некоторых стран и культур сценарий "проигрыш для всех" нередко является полностью приемлемым вариантом.

Наибольшее беспокойство, однако, в перспективе связано с негосударственными субъектами. Абсолютный кошмар наступит тогда, когда способность причинить вред совместится с намерением причинить вред, независимо от цены. Мы еще не достигли этой точки, но страх перед применением террористами кибероружия лежит в сфере возможного. Существуют доступные через интернет комплекты "готово к использованию", которые можно далее развивать, существуют черные рынки нулевого дня и существуют кибернаемники – весьма квалифицированные группы "хакеры напрокат", услуги которых могут быть куплены для кражи денег или

---

[53] Выступление заместителя министра обороны Линна на 28-м ежегодном Международном семинаре-практикуме по глобальной безопасности, Париж, 16 июня 2011 года.

[54] Речь Габора Иклоди на Глобальном форуме AFCEA по вопросам анализа разведывательной информации, Брюссель, 10–11 декабря 2013 года.

промышленных секретов либо, используя практически те же инструменты и методы, совершения массовых нарушений.

1.4 Концепция кибербезопасности, принятая в Организации Объединенных Наций

Хамадун Туре

В данном разделе представлены основы принятой в ООН концепции кибербезопасности. ИКТ играют центральную роль в современном развитии, и безопасность этих систем приобретает все более критическое значение. Развитые экономики весьма сильно зависят от ИКТ, включая важнейшую инфраструктуру, что обусловливает приоритетную актуальность кибербезопасности, и многие страны уже признали это. Для развивающихся стран открывается уникальная возможность построить заведомо безопасную информационную инфраструктуру и благодаря этому сделать качественный скачок в своем развитии.

Однако кибербезопасность еще далеко не получила глобального приоритета и зачастую не упоминается в национальных стратегиях в области ИКТ и развития. Включая кибербезопасность в программы развития и рассматривая это как "средство достижения цели", а не саму конечную цель, ООН пытается изменить сложившуюся ситуацию. В настоящей статье показана существующая в нынешнее время глобальная потребность в кибербезопасности, представлена принятая в ООН концепция развития кибербезопасности, соответствующие внедренные в настоящее время механизмы и краткое описание осуществляемых и планируемых инициатив в области кибербезопасности.

Потребность в глобальной кибербезопасности

ИКТ обладают "преобразующей мощью"[55], которая проникла практически во все отрасли в развитых странах и привела к быстрым преобразованиям в развивающихся странах. Однако повсеместно распространенные компьютерные сети обходятся дорого – целые сектора экономики становятся более уязвимыми для кибератак. Диапазон целей этих угроз широк – от мелкого хулиганства и кражи номера одной кредитной карты до глобальных координируемых атак (например, Conficker).

---

55 Речь Генерального секретаря МСЭ Хамадуна И. Туре на встрече на высшем уровне "Преобразуем Африку", Международный союз электросвязи, 28 октября 2013 года, размещена веб-сайте 24 июля 2014 года.

Преступники действуют, как правило, анонимно[56], что еще более усложняет привлечение к уголовной ответственности. Кроме того, традиционные правоохранительные подразделения располагают ограниченными ресурсами в кибербласти, а злоумышленники зачастую действуют из разных юрисдикций. Эти факторы находятся во взаимодействии в сложной области, которая ставит перед всеми странами проблемы и технического и политического характера: жизненно важно защищать целостность, конфиденциальность и доступность как критически важной информации, так и личных данных.

Ряд развитых стран приняли кибербезопасность в качестве национального приоритета[57]. Имея дело с сетью, разработанной для обеспечения открытости, а не безопасности, страны тратят огромные ресурсы для защиты своих сетей: по оценкам, эти расходы в 2014 году составили более 70 млрд. долл. США[58]. Однако эти расходы сосредоточены в основном в странах с высоким уровнем доходов и представляются недостаточными, учитывая, что злоумышленники постоянно нацеливаются на новые отрасли[59].

Киберугрозы, мотивы которых весьма разнообразны – от финансовой прибыли до политического активизма, могут исходить из практически любой страны и воздействовать на огромное число секторов экономики. Эффективно противостоять угрозам в одиночку невозможно – ни предприятиям, ни государствам. Эти факторы усиливают неотложную потребность в глобальных согласованных усилиях по обеспечению кибербезопасности.

Существует также иная, более широкая причина, обусловливающая потребность в кибербезопасности, выходящая за рамки ставшего привычным лексикона "кибервойн" и "кибератак". Комплексный подход обеспечит защиту и права на информацию, и права на конфиденциальность в киберпространстве, – оба эти права являются основными правами человека, признанными международными договорами. Следовательно, укрепление доверия в этом новом пространстве путем повышения безопасности этого пространства приведет, наряду с активизацией экономического развития, к формированию среды, которая обеспечивает защиту отдельных лиц от несанкционированного вторжения в их информацию. Именно в силу

---

56 Nazli Choucri, Stuart Madnick & Jeremy Ferwerda, Information Technology for Development (2013): "Institutions for Cyber Security: International Responses and Global Imperatives, Information Technology for Development," DOI: 10.1080/02681102.2013.836699

57 "Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy." *Organization for Economic Cooperation and Development,* 2012.

58 "Defending the Digital Frontier." *The Economist*, July 12, 2014.

59 "Hackers Inc." *The Economist*, July 12, 2014.

этих причин международное сообщество должно активизировать усилия, для того чтобы придать кибербезопасности первостепенное значение в глобальном масштабе.

Принятый в ООН подход к кибербезопасности базируется на четырех задачах: 1) защита собственных сетей каждой организации; 2) предоставление (согласованной) помощи Государствам-Членам[60] в целях разработки мер национальной политики в области кибербезопасности и их реализации; 3) включение кибербезопасности в программы развития; и 4) содействие международному сотрудничеству по вопросам кибербезопасности, киберпреступности и защиты прав человека в онлайновой среде – в особенности конфиденциальности информации и доступа к ней. Настоящая статья посвящена главным образом трем последним задачам, так как они в большей степени относятся в целом к "поискам кибердоверия" – теме данной публикации. Ниже рассматривается каждая из этих задач.

ООН считает, что в основе этих трех приоритетных задач глобальной кибербезопасности лежат общие принципы. Во-первых, а также в целях эффективной защиты информационных технологий, ООН выступает за комплексный, "общеправительственный", предусматривающий участие многих заинтересованных сторон подход. Внутренняя деятельность Организации Объединенных Наций должна соответствовать этой доктрине, и переход к "межучрежденческому" подходу, в рамках которого соответствующие структуры координируют свою работу, становится, таким образом, более эффективным и не допускающим дублирования усилий. Во-вторых, учитывая динамичный характер информационных технологий, ООН рекомендует применять гибкие и часто пересматриваемые стратегии, которые в максимально возможной степени являются нейтральными в отношении технологий. Наконец, при выработке политики следует определить приоритет воздействия мер безопасности на другие глобальные приоритетные направления, такие как защита конфиденциальности.

Помощь Государствам-Членам

Учреждения Организации Объединенных Наций в течение длительного времени участвуют в оказании Государствам-Членам помощи по вопросам развития ИКТ. Однако лишь в последнее время кибербезопасность начала приобретать приоритетный характер. Благодаря разработке общесистемной рамочной программы Организации Объединенных Наций по борьбе с киберпреступностью и по обеспечению кибербезопасности и ее одобрению в 2013 году, Координационный совет руководителей системы ООН[61] достиг согласия по ряду общих принципов, определяющих предоставление помощи Государствам-Членам. Эта Рамочная

---

[60] В рамках мандата каждого учреждения и не нарушая национального суверенитета.

[61] См. п. 85 of the CEB Second Regular Session Report for 2013 (November 2013).

программа, которая стала первым шагом на пути к согласованию внутренней деятельности ООН, относящейся к кибербезопасности, рассматривается ниже[62].

Включение кибербезопасности в программы развития

Развитие ИКТ (частью чего является кибербезопасность) рассматривалось в целом как приоритетное направление, не связанное с другими традиционными областями развития. В результате этого другие области представлялись более важными и актуальными по сравнению с областью кибербезопасности. Однако развитие ИКТ не расходится с общими темами устойчивого развития: техническое развитие – это не самоцель, оно открывает перед странами, в особенности перед развивающимися и наименее развитыми странами (НРС) возможность расширения своих возможностей в очень многих экономических сферах, повышая также общественное благополучие и уровень жизни в целом. Существует множество примеров того, как технологии улучшили доступ к воде, образованию, сделали более доступным медицинское обслуживание наряду с ускорением экономического роста и развитием/активизацией международной торговли.

Включение кибербезопасности в число *существующих* приоритетов развития является, следовательно, первоочередным требованием: безопасность и доверие к системам усиливают вероятность их внедрения. Развивающиеся страны и НРС имеют в этом отношении исключительную возможность: ориентируясь на разработку заведомо безопасных компьютерных сетей, они могут обойти системы, на которые уже совершаются атаки. Инвестиции в кибербезопасность могут далее способствовать преодолению так называемого "цифрового разрыва". Система ООН может играть в этом исключительно важную роль, используя существующие международные механизмы для включения аспектов кибербезопасности в программы.

Еще одним глобальным приоритетом является предупреждение возникновения и эскалации киберконфликтов. Невозможно допустить, чтобы проявляемая до сих пор странами сдержанность в реагировании на кибератаки[63] сохранялось в средне- и долгосрочной перспективе. Институт Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР), ведя исследовательскую и образовательную деятельность, стремится внести вклад в предупреждение эскалации конфликта, так как это "[…] служит мостом к формированию необходимой синергии для устранения и смягчения последствий отсутствия безопасности на международном, региональном и местном уровне".

---

62 См. раздел "Механизмы ООН для обеспечения кибербезопасности".

63 Valeriano, B., & Maness, R. C. (2014). "The dynamics of cyber conflict between rival antagonists, 2001-11." *Journal of Peace Research*. doi:10.1177/0022343313518940.

Содействие международному сотрудничеству в области кибербезопасности

Деятельность в онлайновой среде является объектом различного регулирования в рамках юрисдикций, однако при этом интернет, как таковой, остается в основном глобальной сетью. Это в особенности относится к вопросам кибербезопасности, когда атаки и угрозы ежедневно пересекают национальные границы. Примером этого служит, например, Conficker, компьютерный червь, который смог распространиться на 180 стран[64]. Никакая страна в одиночку не сможет решить проблемы кибербезопасности, и Организации Объединенных Наций осуществляет содействие международному сотрудничеству по вопросам кибербезопасности как глобального приоритета.

Применительно к обеспечению доверительных отношений в киберпространстве первоочередное внимание уделяется ООН защите прав человека в онлайновой среде. Особо заметными приоритетами являются неприкосновенность личной жизни и право на информацию. Первому приоритету составляют угрозу различные действия, в том числе постоянные утечки данных, а также недостаточный объем инвестиций в защиту данных. Право на информацию зависит от доступа к безопасным ИКТ, которые обеспечивают свободу выражения мнений и открытый доступ к общедоступному контенту. В программах по защите ИКТ должен учитываться этот конфликт интересов, который, как оказалось, имеет место во внутренней политике многих стран, в первую очередь развитых[65]. Принципы П-О-Д-М, согласно которым интернет должен быть: основан на **п**равах человека; **о**ткрытым; **д**оступным для всех; и формироваться на основе участия **м**ногих заинтересованных сторон, обеспечивают твердую основу для дальнейшей работы в этом направлении. Организация ООН по вопросам образования, науки и культуры (ЮНЕСКО) как учреждение ООН, обладающее большим опытом защиты прав человека во всем мире, представила это более широкое видение кибербезопасности в качестве приоритетного направления устойчивого развития.

С учетом преобладающего участия частных субъектов в экономике на базе интернета и даже в управлении самой сетью, следует прилагать усилия для достижения такой защиты в координации с заинтересованными сторонами, включающими помимо правительств отраслевые организации, техническое сообщество и гражданское общество. Такое расширенное сотрудничество особенно важно в отношении юридических расследований, в которых взаимная помощь может быть выгодна всем участвующим сторонам.

---

64 "Conficker." ShadowServer. Shadowserver Foundation, n.d. Web. 4 Nov. 2013.

65 См. выше сноску 2.

Основные руководящие указания по кибербезопасности

Превращение киберпространства в многогранную область международных коммуникаций принесло, наряду с бесчисленными преимуществами более соединенного мира, серьезные угрозы безопасности и стабильности Государств – Членов ООН. Конфиденциальность информации, компьютерные системы, важнейшая инфраструктура и сетевые услуги – все это уязвимо перед атаками с использованием интернета, которые регулярно происходят по всему миру. Для обеспечения безопасности киберпространства в этих условиях[66] требуется подход, который:

- является всесторонним (или "общегосударственным"), поскольку в предотвращении[67], обнаружении, смягчении последствий и расследовании кибератак участвует множество правительственных и частных организаций;
- включает заинтересованные стороны в области ИКТ, в том числе директивные органы, поставщиков услуг интернета и электросвязи, технические организации и неправительственные организации, занимающиеся защитой прав человека (или "гражданское общество");
- содействует гибкой и динамичной политике, которая удовлетворяет требованиям постоянно меняющегося спектра технологий, обеспечивая возможность реагирования на неизвестные ранее угрозы и уязвимости ("нулевого дня") и при этом не сдерживая инновации; и
- соблюдает права человека, в частности право на неприкосновенность личной жизни и доступ к информации.

Механизмы Организации Объединенных Наций для обеспечения кибербезопасности

Целый ряд заметных рамочных программ ООН в области кибербезопасности, имеющих мировое значение, уже введен в действие, в том числе Общесистемная рамочная программа ООН по борьбе с киберпреступностью и по обеспечению кибербезопасности; Направление деятельности С5 "Укрепление доверия и безопасности при использовании ИКТ" Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО); и Сеть информации, коммуникации и технологий (Сеть ИКТ). Каждая из этих программ будет описана в следующих подразделах. В данном разделе представлены также избранные механизмы обеспечения безопасности, над которыми в настоящее время ведется работа в системе ООН.

---

66 Данный раздел не является исчерпывающим описанием руководящих указаний ООН в области кибербезопасности; он является скорее базовым обзором общих тенденций, выявленных в рассмотренных публикациях.

67 Включая создание возможностей на уровне пользователя.

Общесистемная рамочная программа ООН по обеспечению кибербезопасности

В рамках усилий по ослаблению киберугроз, предпринимаемых в настоящее время ООН, в Общесистемной рамочной программе ООН по борьбе с киберпреступностью и по обеспечению кибербезопасности представлено руководство для всех ее учреждений, стремящихся реагировать на обеспокоенность Государств-Членов относительно этих проблем, и ставится задача по усилению координации их действий в целях укрепления доверия и безопасности в киберпространстве.

Преступная деятельность в интернете варьируется в широких пределах по своему масштабу и регулярности. В рамочной программе предпринята попытка рассмотреть существенную долю этих угроз и с этой целью установить основные принципы, которым должны следовать все учреждения ООН в рамках своих соответствующих мандатов. Эти общие усилия ООН направлены на предотвращение и своевременное обнаружение преступлений, укрепление внутренних возможностей стран, эффективное сдерживание и содействие отправлению правосудия в отношении киберпреступной деятельности. Рамочная программа включает технические аспекты оказания помощи Государствам-Членам и аспекты, связанные с созданием потенциала, при этом используется всесторонний подход для повышения информированности и расширения возможностей реагирования на киберугрозы.

Как определено в Рамочной программе[68], под кибербезопасностью имеется ввиду набор документов, практических подходов, стратегий и технологий, используемых для "[…] создания и сохранения свойств безопасности" соответствующих организаций, информации, систем и ресурсов. От чего защищает кибербезопасность? Помимо обеспечения большего доверия к информационным технологиям, кибербезопасность ограждает от преступной деятельности, связанной с компьютерами, или киберпреступности[69]: комплекса "[…] тем, [которые] включают преступления против конфиденциальности, целостности и доступности компьютерных данных" и инфраструктуры; и комплекса "… [преступных] деяний, связанных с компьютерами", а также деяний, связанных с данными.

Принципы, относящиеся к кибербезопасности и киберпреступности

В целях установления широкой сферы применения Общесистемной рамочной программы ООН этот документ выстроен вокруг семи широких принципов, которые удобнее перевести в конкретные стратегии и обобщить следующим образом:

1. Учреждения ООН должны помогать Государствам-Членам во всестороннем урегулировании киберинцидентов, в том числе путем обеспечения

---

68 В Рамочной программе используется определение Международного союза электросвязи в том виде, как оно изложено в Рекомендации МСЭ-Т X.1205.

69 Как определено в Рамочной программе.

технической поддержки в области уголовного правосудия и укрепления международного сотрудничества.

2. При рассмотрении потребностей Государств-Членов должны учитываться собственные мандаты учреждений ООН и следует добиваться сотрудничества с другими соответствующими организациями ООН.
3. Во всех программах в области кибербезопасности и киберпреступности должны соблюдаться права человека и принцип верховенства закона.
4. При выполнении программ ООН должна, по возможности, оказываться помощь Государствам-Членам в применении основанных на фактах подходов при проведении оценки уровней преступности и рисков.
5. По возможности, следует продвигать "общегосударственную" модель реагирования, которая включает все основные заинтересованные стороны на национальном уровне, а также негосударственных субъектов, таких как НПО, академические организации и техническое сообщество.
6. Поддержка Государств-Членов должна быть направлена на укрепление соответствующих официальных и неофициальных механизмов международного сотрудничества по вопросам кибербезопасности и киберпреступности.
7. При необходимости, для обеспечения эффективного реагирования на киберугрозы, следует поощрять сотрудничество государственного и частного секторов в Государствах-Членах, а также согласование и внедрение технической политики, стандартов безопасности и руководящих указаний по безопасности на региональном и международном уровнях.

Таким образом, в основе Рамочной программы лежит помощь Государствам-Членам: в ней прилагаются усилия к совершенствованию кибербезопасности и превращению интернета в более безопасное пространство, внушающее больше доверия. В Рамочной программе изложены рекомендации по реализации вышеупомянутых принципов и эффективному предоставлению такой помощи. Эти руководящие указания можно отнести к трем категориям: правовые и политические меры, техническая помощь и механизмы реализации.

Техническая помощь

В столь технической, по сути, области, как киберпространство, считаются важными создание потенциала и профессиональная подготовка в области базовых навыков кибербезопасности в Государствах-Членах. В Рамочной программе рекомендуется проведение странами полной оценки внутренних технических возможностей в качестве неотъемлемой отправной точки и выработка национальной стратегии кибербезопасности. Более конкретно, техническая помощь, оказываемая учреждениями ООН, может включать: технические публикации по вопросам

киберпреступности и ее экономической составляющей; механизмы обмена информацией (передовой опыт и другие виды поддающихся обобщению знаний); подготовку в области компьютерного экспертно-технического анализа и других навыков расследования киберпреступлений, включая обучение конечных пользователей безопасному использованию компьютера и сетей; сотрудничество с частными поставщиками услуг интернета (ПУИ) и другими соответствующими заинтересованными сторонами в области сбора и анализа данных; реагирование на компьютерные инциденты, включая создание постоянных учреждений по урегулированию инцидентов (например, национальных Групп реагирования на компьютерные инциденты – CIRT) и "центральных координационных бюро для рассмотрения запросов из-за границы".

Направление деятельности С5 ВВУИО

Как указано в итоговых документах ВВУИО (2003 г.)[70] и уточнено в ходе мероприятия высокого уровня ВВУИО+10 (2014 г.), в Направлении деятельности С5 ВВУИО акцентируется внимание на укреплении доверия и безопасности при использовании ИКТ, и ответственность за содействие его реализации была возложена на МСЭ. В 2007 году МСЭ разработал Глобальную программу кибербезопасности (ГПК) "[…] в целях обеспечения основы для координации и решения вопросов международных ответных мер в связи с возрастающими проблемами обеспечения кибербезопасности" совместно с Государствами-Членами и другими соответствующими заинтересованными сторонами. В связи с этим МСЭ установил партнерские отношения со всеми заинтересованными сторонами в мире для развития кибербезопасности и, в том числе, публикации руководящих указаний по выработке национального политического курса в области кибербезопасности[71], оказания технической помощи Государствам-Членам в развитии потенциала на национальном уровне, а также содействия всестороннему обсуждению вопроса о необходимых технических стандартах для повышения безопасности.

Сеть ИКТ

Сеть ИКТ, являющаяся механизмом Координационного совета руководителей системы ООН, объединяет связанные с ИКТ возможности многих учреждений ООН по выработке политики. Она служит целям координации и является форумом для разработки и реализации стратегии в области ИКТ. Однако для данной публикации большее значение представляет ее Группа особых интересов в сфере безопасности

---

70 Всемирная встреча на высшем уровне по вопросам информационного общества http://www.itu.int/wsis/index.html, последние изменения от 13.10.2014 г.

71 ITU National Cybersecurity Strategy Guide, September 2011.

информации, которая изучает вопросы, касающиеся кибербезопасности", […] с помощью выступлений экспертов и докладов об исследовании конкретных ситуаций, [а также рассмотрения] межучрежденческих направлений деятельности, включая реагирование на инциденты, информационную безопасность и политику в области информации, а также информированность в вопросах информационной безопасности"[72].

Ведущаяся деятельность

Как признается и Государствами – Членами ООН, и КСР[73], необходимо сосредоточить усилия системы ООН на вопросах кибербезопасности и киберпреступности. После одобрения Общесистемной рамочной программы ООН по борьбе с киберпреступностью и по обеспечению кибербезопасности в 2013 году, Генеральный секретарь ООН Пан Ги Мун призвал МСЭ вместе с ЮНЕСКО, ЮНОДК, ПРООН и ЮНКТАД и в тесном сотрудничестве с Комитетом высокого уровня по вопросам управления (КВУУ), Комитетом высокого уровня по программам (КВУП) и Группой ООН по вопросам развития (ГООНВР) разработать для всей системы всеобъемлющую и последовательную стратегию решения соответствующих вопросов для обсуждения ее на второй регулярной сессии КСР в ноябре 2014 года[74], и в этом направлении ведется работа.

Выводы

Существует глобальный консенсус по вопросу о необходимости комплексного глобального реагирования на вопросы кибербезопасности. ООН занимается решением этих вопросов, используя всестороннюю гибкую и динамичную модель с участием многих заинтересованных сторон и при соблюдении прав человека. Согласие в отношении концепции кибербезопасности все еще не достигнуто. Несмотря на это в работе учреждений ООН присутствуют некоторые общие элементы и тенденции, которые подчеркивают, что в последнее время кибербезопасность все чаще выступает в качестве глобального приоритета. Сегодня признается, что обеспечение безопасности киберпространства является всеобщей потребностью, которая оказывает очевидное воздействие на социально-экономическое развитие, и при этом также важно обеспечивать баланс противоположных интересов и уважать национальный суверенитет. Как признают Шукри и соавторы[75], перспективы

---

72 Группа особых интересов в сфере безопасности информации. Координационный совет руководителей системы ООН, 2014 г. веб-публикация от 22 июля 2014 г.

73 "Action on Cybersecurity/Cybercrime and Policies on Information." UN – CEB, 21 Nov. 2011. Web. 22 July 2014.

74 См. пункт 85 Доклада второй регулярной сессии КСР, ноябрь 2013 г.

75 См. выше сноску 2.

кибербезопасности представляются весьма радужными: "Несмотря на то, что существующая система [международных] институциональных договоренностей [по кибербезопасности] обнаруживает признаки слабости, также верно, что уровень организации и сотрудничества неуклонно возрастает".

Эта позитивная тенденция является дополнительным стимулом к международному сотрудничеству в области кибербезопасности; с учетом глобального характера интернета, только те усилия, которые имеют всемирный (или почти всемирный) охват, могут быть эффективными в обеспечении безопасности киберпространства. Затраты, связанные с прерыванием обслуживания в результате кибератак, могут быть весьма высоки, особенно в важнейших секторах, таких как энергоснабжение или финансы, однако выгоды от инвестирования в кибербезопасность существенно их перевешивают. Эти расчеты относятся к развитым странам с исключительно взаимоувязанной инфраструктурой. С другой стороны, развивающиеся страны добиваются исторической возможности скачкообразного развития, и отнесение кибербезопасности к числу первоочередных задач может несомненно повысить эти шансы.

Данные изменения воплотятся в жизнь только в том случае, если кибербезопасность станет действительно глобальным приоритетом. ООН, имеющая существенный опыт развития в новых областях, больше всех подходит на роль глобальной содействующей организации для международных усилий в области кибербезопасности; участие в них может принести большой выигрыш всем – государствам, отраслевым организациям и гражданскому обществу.

Глава II: Способность к восстановлению в киберсреде

Введение

В феврале 2005 года Консультативный комитет по информационным технологиям при Президенте США выпустил призыв к действиям[76] с целью укрепления безопасности в киберпространстве[77] в знаковом отчете под названием "Кибербезопасность: кризис в установлении приоритетов". Соответствующая тема, включенная в список "14 крупных задач XXI века", была опубликована Национальной академией инженерных наук США в 2008 году. В последние годы во многих других источниках также рассматривается проблема обеспечения кибердоверия в будущем цифровом мире.

---

[76] Консультативный комитет по информационным технологиям при Президенте "Cyber Security: A Crisis of Prioritization" (февраль, 2005 г.).

[77] Национальная академия инженерных наук: "Grand Challenges for Engineering", http://www.engineeringchallenges.org/cms/challenges.aspx.

С того времени зависимость человечества от преимуществ цифровой эпохи продолжает расти стремительными темпами, по мере того как вычислительные и коммуникационные устройства и системы становятся все более распространенными и значимыми практически для каждого аспекта нашей повседневной жизни.

Поэтому сохранение кибермира и укрепление способности к восстановлению имеют решающее значение для преодоления растущей угрозы кибератак, которые способны нанести серьезный ущерб и причинить разрушения в особо крупных масштабах.

Все более широкое использование сенсорных технологий, киберфизических систем, облачных услуг, больших данных и адаптивных интеллектуальных систем[78] существенно расширит возможности ИКТ и влияние на повседневную жизнь по мере неизбежного перехода к интернету вещей.

Эта тенденция обусловлена не только развитием технологий, но и постоянным новым рыночным спросом и спросом на продукцию. Расширение киберинфраструктуры и киберуслуг предоставит более широкие возможности и преимущества, но и приведет к дополнительным уязвимостям и новым угрозам, способным подорвать личную и общественную безопасность и защищенность наших обществ.

Эта проблема крайне актуальна не в последнюю очередь потому, что доверие к цифровому веку и даже наше общее благосостояние во многом зависят от нашей способности выявлять широкий круг киберугроз и справляться с ними. На основе тщательного анализа и оценки уязвимостей и рисков необходимо выработать соответствующие меры, чтобы гарантировать кибербезопасность, или хотя бы надлежащую способность к восстановлению, в особенности применительно к важнейшим инфраструктурам, таким как системы энерго- и водоснабжения, транспортные, медицинские и финансовые системы[79].

Источники потенциального риска для киберстабильности и кибербезопасности включают усложнение и все более широкое использование инфраструктур и услуг ИКТ. Еще более серьезными являются угрозы, связанные с внешними событиями, такими как стихийные бедствия или атаки, осуществляемые правительствами, преступными организациями или отдельными лицами. Исследования показали, что даже проектировщики, операторы и пользователи систем могут преднамеренно или непреднамеренно стать одним из основных источников уязвимости ИКТ. В связи с этим должны быть решены основные научно-технические проблемы, связанные с

---

78 Markus Luckey Gregor Engels: "High-Quality Specification of Self-Adaptive Software Systems". In: Proceedings of the 8th International Symposium on Software Engineering for Adaptive and Self-Managing Systems. ACM (New York, NY, USA), SEAMS '13, pp. 143–152; (2013).

79 Указ Президента США № 13636: "Improving Critical Infrastructure Cybersecurity" (февраль, 2013 г.): http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

вопросами "сложности, чрезвычайных ситуаций, способности к восстановлению" в киберпространстве.

Прежде всего, в настоящей главе разъясняются термины, которые касаются сложности ИКТ, вытекающих из этого киберрисков и неожиданного поведения системы, а также растущей потребности в надлежащих методиках укрепления способности к восстановлению в киберсреде. Далее, в ней излагаются многочисленные потенциальные источники киберрисков – от физических, технических или связанных со средой ошибок и отказов до организационных, институциональных или законодательных причин – и обсуждаются с точки зрения компьютерных и инженерных наук методики выявления и анализа киберрисков, а также укрепления способности к восстановлению, относящиеся к уровням вплоть до информационного. В следующих главах более подробно рассматриваются проблемы, связанные со способностью к восстановлению, применительно к приложениям "больших данных" и "облачных вычислений", а также потребности способных к восстановлению систем киберуправления. Наконец, в эту главу включены материалы, касающиеся способности к восстановлению в киберсреде, в которых отражена точка зрения частного сектора, рассматриваются основные киберриски нетехнического характера и предлагается международная нормативно-правовая база первой необходимости для противодействия существующим рискам за пределами области защиты данных.

В главе 2.4 рассматриваются основные киберриски нетехнического характера и предлагается международная нормативно-правовая база первой необходимости для противодействия существующим рискам за пределами области защиты данных.

2.1 Основы обеспечения способности к восстановлению в киберсреде

Аксель Лехман

Термины

Как уже было указано, реальная проблема при разработке СВМ заключается в повышении сложности цифрового мира, который влияет на повседневную общественную и личную жизнь. В целом **сложность той или иной (цифровой) системы** зависит от количества и функциональных возможностей ее компонентов, которые определяют пространство состояний системы.

Суперкомпьютеры обеспечивают высочайшие уровни производительности, и, как ожидается, в следующем десятилетии их пиковая производительность составит порядка 1000 петафлопс – 100 квадриллионов операций с плавающей запятой в

секунду[80]. Киберфизические системы (в основном невидимые) и встроенные микровычислительные устройства обеспечивают только узкоспециализированные и ограниченные вычислительные возможности.

Расширенные возможности установления соединений между разнообразными системами позволяют формировать так называемые "системы систем" (используемые, например, для регулирования систем энергоснабжения, связи и управления движением)[81]. Хранение информации является еще одной важной глобальной услугой, которая должна учитываться применительно к кибердоверию; технологии хранения развиваются даже быстрее, чем компьютерные технологии (постоянно увеличивающаяся емкость запоминающих устройств при существенно уменьшающейся стоимости).

При увеличении числа компонентов и возможностей системы, а также ряда систем, соединенных в рамках масштабируемой "системы систем", общая сложность требующей управления системы растет экспоненциально.

Эти непрерывное совершенствование техники требует особо надежных методов проектирования, разработки и обеспечения качества, чтобы гарантировать стабильность и готовность системы, а также требует методик укрепления способности к восстановлению в случае нежелательных ситуаций[82] и кибердоверия. Все более широкое применение формальных методов описания и проектирования системы может обеспечить возможность обнаружения и недопущения определенных (небезопасных или критических) состояний системы при условии реализации надлежащих мер выявления и предотвращения. Однако события или опасности, которые не могли быть предусмотрены в процессе проектирования, могут привести к неожиданному или непредвиденному поведению системы, которое может быть трудно или даже невозможно контролировать или исправить. В худшем варианте система может выйти из строя и не подлежать восстановлению до рабочего состояния. В связи с этим должны быть разработаны и реализованы надлежащие методы укрепления способности к восстановлению.

Данные угрозы, уязвимости и риски должны быть выявлены, проанализированы, оценены, и должны быть разработаны меры противодействия. Проектирование цифровых систем с использованием формально доказанных методов проектирования и обеспечения устойчивости к сбоям существенно повысит их надежность и управляемость, но не устранит полностью непредвиденное поведение, особенно в

---

80 Экзафлопсные вычисления: см.: http://en.wikipedia.org/wiki/Exascale_computing.

81 Mo Jamshidi: "System-of-systems engineering: a definition"; In: IEEE SMC; (2005).

82 "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; Published by Ashgate Publishing Limited (2006).

рамках конфигурации системы систем. Поэтому должны быть изучены и реализованы методы и процедуры исправления с целью укрепления **способности систем и процессов к восстановлению** как важного шага к установлению доверия к ним и к киберпространству в целом.

Согласно определению, данному Ритхоллом[83], "[…] способность к восстановлению – это возможность организации (системы) поддерживать стабильное состояние или быстро возвращаться в него, обеспечивая продолжение работы во время и после крупных неполадок или при наличии постоянных существенных нагрузок". На Всемирном экономическом форуме 2012 года была создана инициатива "Установление партнерских отношений для укрепления способности к восстановлению" и были сформулированы некоторые "Принципы и руководящие указания относительно рисков и обязанностей в гиперсоединенном мире"[84]. С учетом огромного разнообразия пользователей-людей, проектировщиков, операторов, цифровых устройств и систем, которые образуют этот сложный цифровой мир, а также результатов исследований, которые показали, что наиболее уязвимыми объектами в нем являются люди, их деятельности должно уделяться особое внимание в контексте мер по укреплению доверия.

Выявление и классификация киберрисков

В мире, где люди столь зависимы от киберресурсов, при анализе рисков и способности к восстановлению в киберпространстве должен учитываться целый ряд аспектов, охватывающих как одушевленных субъектов, так и разнообразие и сложность цифрового века. Спектр ресурсов киберпространства включает от глобальных цифровых инфраструктур и услуг, которые могут использоваться во всем мире, до отдельных вычислительных или киберфизических устройств.

Также, применительно к деятельности людей в киберпространстве, например проектировщиков, разработчиков или пользователей, необходимо устанавливать различия между их ролями и возможностями в использовании цифровых систем в качестве либо осведомленных лиц (инсайдеров), либо сторонних лиц. В терминах иерархии, а также для целей классификации средств выявления, анализа и предотвращения киберрисков можно различать следующие уровни или слои абстракции. В связи с тем, что нарушения и недоработки, возникающие на более низких уровнях, могут оказать существенное влияние на поведение и работу системы

---

83 John Wreathall: "Properties of Resilient Organizations: An Intitial View"; In: Resilience Engineering – Concepts and Precepts, Ashgate Publishing Limited (2006).

84 Всемирный экономический форум: "Partnering for Cyber Resilience"; February 2013 Newsletter – Davor Special Edition; http://www3.weforum.org/docs/WEF_RRHW_PartneringCyberResilience_NewsletteFebruary_2013.pdf (2013).

на более высоких уровнях, при анализе общего риска и оценке риска должны учитываться все приведенные ниже факторы как необходимое условие разработки методик укрепления способности системы к восстановлению[85],[86]:

- глобальный уровень;
- корпоративный/институциональный/личный уровень;
- информационный уровень;
- технический уровень;
- физический уровень.

Анализ киберрисков и способность к восстановлению в киберсреде с точки зрения компьютерных и инженерных наук

Для разработки эффективных методик анализа киберрисков и укрепления способности к восстановлению в киберсреде должны быть выявлены основные источники киберрисков на каждом из указанных выше уровней. На втором этапе должны быть проведены тщательные анализ и оценка любых побочных эффектов (зависимостей), так как ошибка, сбой, отказ или проникновение на более низком уровне может оказать влияние на функциональные возможности, надежность или конфиденциальность и безопасность на более высоких уровнях. Для этого используются графы зависимости[87], чтобы обнаружить взаимозависимости с помощью прямого и обратного прохождения уровневых путей навстречу друг другу, что позволяет определить причины неправильного функционирования, сбоев, отказов, утечек или повреждений данных.

Как показано на рисунке 1, ниже, на каждом уровне обеспечиваются определенные возможности, функциональные возможности или услуги (cx), которые включают или используют атрибуты более низкого уровня, обозначенные направленными дугами. Пунктирные дуги обозначают, что для реализации каждой возможности (cx) требуется соблюдение определенных стандартов, регламентов или правил. На Рисунке 1 выявлена недоработка на корпоративном уровне; ее возможной причиной является ошибка, сбой или проникновение в данном узле или в узле более низкого уровня. С помощью прохождения структуры графа (прямая и обратная последовательность

---

85 "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; Published by Ashgate Publishing Limited (2006).

86 Lorenzo Strigini: "Fault tolerance and resilience: meanings, measures and assessment"; In: K. Wolter et al. (eds.), Resilience Assessment and Evaluation of Computing Systems, Springer-Verlag, Berlin Heidelberg (2012).

87 Algirdas Avizienis, Jean-Claude Laprie, Brian Carl: "Basic Concepts and Taxonomy of Dependable and Secure Computing"; IEEE Transactions on Dependable and Secure Computing (2004).

прохождения структуры графа) можно определить места расположения потенциальных источников ошибки, сбоя или отказа.

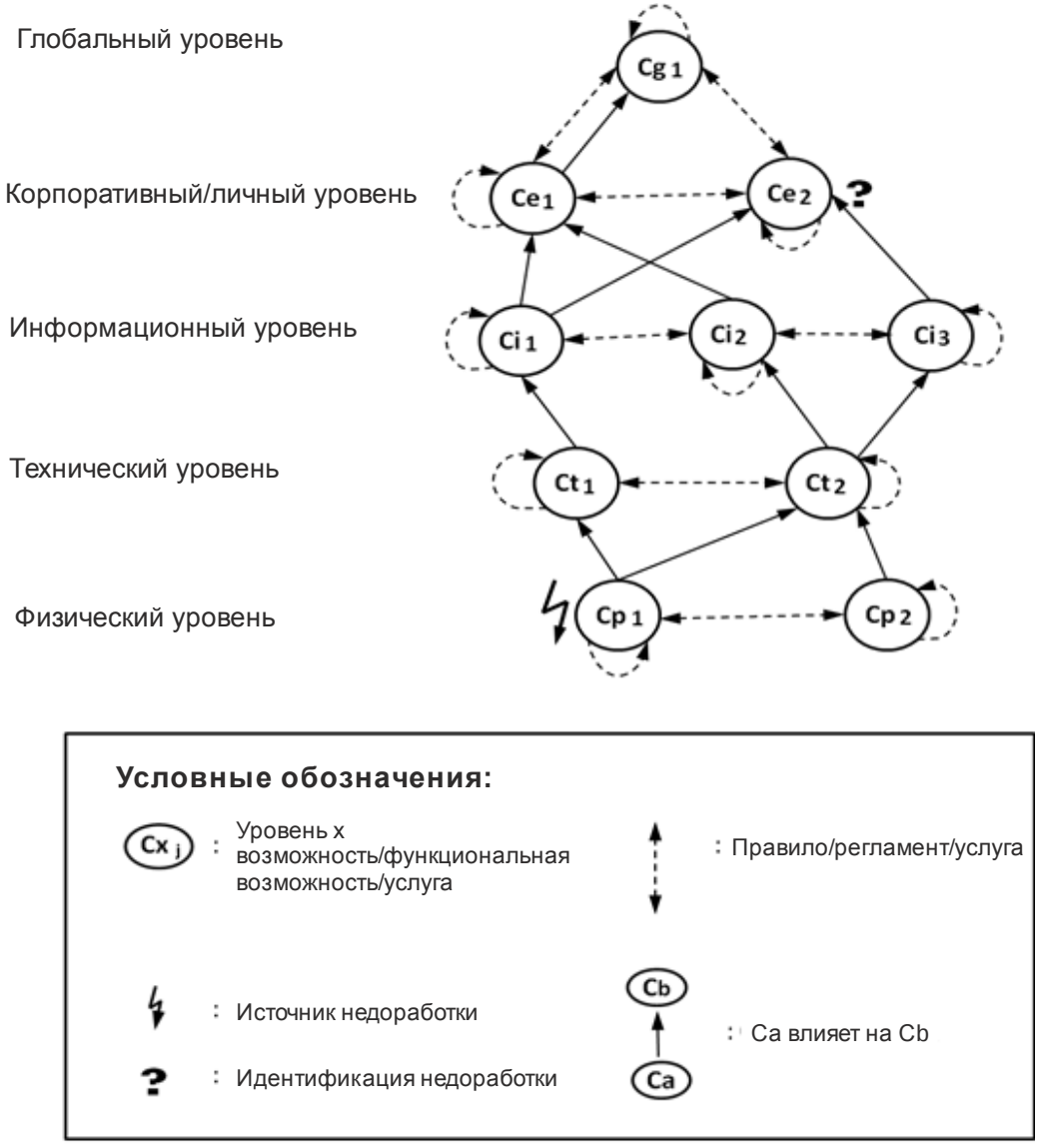

Рисунок 1: Пример графазависимости

Как уже было указано, стремительное развитие ИКТ обеспечивает существенные технические достижения, но в тоже время создает новые источники и причины киберрисков, которые затрагивают стабильность и безопасность в киберпространстве. Помимо физических и технических недоработок, основные источники киберрисков коренятся в тенденции к виртуализации вычислительных и коммуникационных ресурсов, а также ресурсов хранения, что обусловлено спросом сообщества пользователей на повышенную производительность, надежность и рентабельность. Об этой тенденции свидетельствует стремительное развитие технологий, таких как большие данные, облачные вычисления и облачные средства на основе модели "программное обеспечение как услуга" (SaaS)[88], системы систем[89] и "гиперсети"[90].

Это развитие технологий также сопровождается появлением новых вопросов кибербезопасности, касающихся неприкосновенности личной жизни, конфиденциальности и аутентичности. Помимо неправомерного использования данных и инфраструктур ИКТ, манипуляций с ними и их повреждения эти технологии влекут за собой новые риски несанкционированного сбора, использования и объединения персональных и других конфиденциальных данных. Опасность, уже ставшая в некоторых случаях реальностью, заключается в том, что многочисленные виды собственных данных отдельных лиц, организаций и даже государств становятся "прозрачными", и это подрывает доверие к киберпространству.

В общем виде риски можно рассчитать по формуле:

Риск = Вероятность x Последствия

С технической точки зрения киберриски могут быть вызваны ошибками проектирования, сбоями и отказами цифровых компонентов в процессе работы, неправильным функционированием или непредвиденным поведением системы в "гиперсетевых" системных конфигурациях. Кроме того, риски могут возникать в связи с ошибочным или противозаконным использованием цифровых систем, а также из-за внутренних атак, действий пользователей и даже в результате неожиданных инцидентов или событий в окружающей среде. Для сведения к минимуму этих связанных с ИКТ рисков необходимо попробовать использовать более точную формулу для анализа рисков: ИКТ-риск = f (Угроза, Уязвимость, Ресурс).

В контексте ИКТ уязвимость системы ИКТ связана со слабыми сторонами ее проектирования и реализации или допущенными при этом недоработками, или же содержащими ошибки приложениями, которые могут вызвать сбой, уменьшение

---

88 Nicolas Gold, Andrew Mohan; Clair Knight, Malcolm Munro: "Understanding Software-Oriented Software"; In: IEEE Software (2004).

89 Mo Jamshidi: "System-of-systems engineering: a definition"; In: IEEE SMC (2005).

90 "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; Published by Ashgate Publishing Limited (2006).

возможностей, неправильное функционирование компонента системы или даже выход системы из строя. Такие уязвимости требуется вначале выявить и классифицировать, прежде чем рассматривать возможные варианты устранения. Для этого после осуществления оценки рисков, связанных с ИКТ, должны быть установлены приоритеты уязвимостей инфраструктуры и услуг ИКТ и соответствующих мер противодействия. Далее можно провести количественный анализ рисков, например, по формуле:

ИКТ-риск = ((Уязвимость x Угроза / Оценка меры противодействия) x Ценность ресурса.

Необходимым условием разработки методики укрепления способности к восстановлению систем ИКТ является проведение анализа надежности и готовности, в ходе которого должны быть рассмотрены следующие общие методы повышения надежности и готовности системы[91]:

- *Предотвращение сбоев* – не допустить возникновения ошибок и сбоев за счет тщательного проектирования и реализации;
- *Устранение сбоев* – обнаружить наличие ошибок, которые могут привести к сбою или даже отказу, путем применения методов тестирования, верификациии и валидации;
- *Устойчивость к сбоям* – обеспечить резервирование (например, путем дублирования ресурсов и/или использования различных вариантов реализации), с помощью которого можно маскировать и исправить сбои в случае их возникновения;
- *Прогнозирование сбоев/отказов* – проанализировать и оценить последствия сбоев, которые могут привести к отказу системы, а также последствия функционирования системы[92].

С точки зрения специалиста-аналитика графы зависимости (аналогичные приведенному на Рисунке 1) или блок-схемы надежности являются простыми методами анализа эффектов и побочных эффектов, связанных с ошибками, сбоями, отказами, а также конкретными мерами противодействия, указанными выше[93].

Помимо уязвимостей, связанных с ИКТ, применительно к кибердоверию должны учитываться и другие угрозы, вызванные недоработками. "Угроза – это потенциальная

---

91 Algirdas Avizienis, Jean-Claude Laprie, Brian Carl: "Basic Concepts and Taxonomy of Dependable and Secure Computing"; IEEE Transactions on Dependable and Secure Computing (2004).

92 Там же.

93 Там же.

опасность, при которой уязвимость может быть использована для нарушения безопасности и причинения при этом вреда. Поэтому должны быть учтены и оценены дополнительные угрозы, которые обусловлены действиями пользователя-человека над ресурсами системы, инцидентами, стихийными бедствиями или другими неожиданными внешними событиями"[94].

Представляющие угрозу действия человека могут осуществляться либо преднамеренно (например, инсайдерами, хакерами) или непреднамеренно, в результате работы или поведения пользователя. При анализе рисков следует выявить наиболее вероятные действия человека, причиняющие вред, и проанализировать возникающие в связи с этим уязвимости. Помимо уязвимостей и угроз при анализе киберрисков должно учитываться их влияние на возможности и ресурсы системы, а также ценность соответствующих ресурсов.

При развитии способности к восстановлению в киберсреде должны учитываться следующие подходы[95]:

- Предотвращение недоработок – не допустить возникновения неточностей, таких как ошибки, сбои и отказы на физическом и техническом уровнях за счет тщательного проектирования, реализации и работы системы и процедур эксплуатации; на более высоких уровнях этого можно добиться, следуя признанным уровневым стандартам, регламентам или правилам поведения.
- Устранение недоработок – обнаружить наличие недоработок, которые могут привести к сбою, отказу, неправильному функционированию или неправомерному использованию, путем применения методов тестирования, верификации и валидации.
- Устойчивость к недоработкам – обеспечить резервирование, например, путем дублирования ресурсов и услуг, а также использования различных вариантов реализации, с помощью которого можно маскировать или исправить недоработки в случае их возникновения.
- Прогнозирование недоработок – изучить уязвимости в правдоподобных сценариях с помощью масштабной программы имитационного моделирования, анализа соответствующих рисков и оценки последствий реализации методик укрепления способности к восстановлению в данном контексте.

---

94 Lorenzo Strigini: "Fault tolerance and resilience: meanings, measures and assessment"; In: K. Wolter et al. (eds.), Resilience Assessment and Evaluation of Computing Systems, Springer-Verlag, Berlin Heidelberg (2012).

95 Там же.

Для разработки общей методики укрепления способности к восстановления на основе этого анализа рисков и надежности дополнительно требуются механизмы исправления и восстановления, обеспечивающие возможность полного самостоятельного восстановления системы из недоступного состояния, состояний с ухудшенными рабочими характеристиками или после проникновения. Большинством природных или биологических систем разработаны механизмы самоизлечения или самостоятельного изменения структуры. Что касается технических систем, например биоподобных процессов или организаций, называемых органическими вычислительными возможностями, соответствующие методы маскировки, исправления и восстановления должны быть изучены и предопределены на этапе проектирования системы. Научные исследования в области органических вычислений и коммуникаций посвящены таким биоподобным методам, которые могут повысить способность к восстановлению систем ИКТ и киберфизических систем, т. е. принципам реализации автономных цифровых X-систем (X заменяется, например, словами "самозащищающихся", "самоизлечивающихся", "самооптимизирующихся" и самоконфигурирующихся"[96]. На основе результатов исследований в таких областях, как техника представления знаний или добыча данных сформировались принципы проектирования интеллектуальных систем, которые могут применяться для выявления и оценки постоянного риска, а также для осуществления предсказуемых действий, обеспечивающих способность системы к восстановлению.

Ниже приводится пример зависящих от уровня мер предотвращения сбоев, неправильного функционирования, отказов или нарушений и восстановления после них, а также мер по укреплению способности к восстановлению в киберсреде с точки зрения разработки компьютерной техники[97],[98],[99]. Эти меры расположены в порядке возрастания уровня:

---

96 "Organic Computing"; Ed. Rolf Würtz; In: Springer series Understanding Complex Systems; Springer (2008).

97 Yue Yu, Michael fry, Alberto Schaeffer-Filho et.al.: "An Adaptive Approach to Network Resilience: Evolving Challenge Detection and Mitigation"; In: 8th IEEE Internat. Workshop on the Design of Reliable Communication Networks (2011).

98 Dorothy Reed, Kailash Kapur, Richard Christie: "Metzhodology for Assessing the Resilience of Networked Infrastructure"; In: IEEE Systems Journal, Vol. 3 No. 2 (2009)

99 Piotr Cholda, Anders Mykkeltveit et. al.: "A Survey of Resilience Differentiation Frameworks in Communication Networks"; In: IEEE Communications, Surveys, Vol.9 No.4 (2007)

- на физическом уровне – ограничения по использованию материалов и устройств только в соответствии с предварительно определенными условиями окружающей среды (например, по температуре, излучению). Кроме того, можно реализовать резервирование с использованием других возможных материалов, дополнительных процессов эксплуатации и т. д. также путем использования различных вариантов реализации компонентов;
- на техническом уровне – резервирование вычислительных устройств по схеме n из m, принципы передачи и кодирования данных с избыточностью или использование различных, но стандартизованных протоколов безопасной передачи дает возможность не только избежать распространения сбоев, но и обеспечить саморегулирование. Кроме того, мерами технического уровня, позволяющими избежать распространения сбоев, повысить надежность системы и обеспечить способность к восстановлению, являются диверсификация, например использование различных вариантов реализации вычислительных алгоритмов, различных вычислительных узлов, или применение разных принципов хранения[100];
- на информационном уровне – цель заключается в "сохранении конфиденциальности, целостности и доступности информации. Кроме того, могут также включаться другие свойства, например аутентичность, возможность учета и предотвращение отказа от авторства" – ИСО/МЭК 27000[101]. К числу мер относятся, например, избыточное кодирование или использование надежных алгоритмов шифрования/дешифрования или протоколов безопасной передачи данных для предотвращения сбоев, неправомерного использования или повреждения; что касается инструментов, то на корпоративном/личном уровне могут быть установлены системы и сети SCADA (Диспетчерский контроль и сбор данных)[102], чтобы следовать сложившемуся передовому опыту, стандартам, правилам и ограничениям в отношении деловой деятельности, делового процесса и безопасности, а также внутренним кодексам поведения[103];

---

100 Министерство энергетики США: "21 Steps to Improve Security of SCADA Networks" (2011); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf.

101 Стандарт ИСО/МЭК 27000: Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология (2014 г.)

102 Министерство энергетики США: "21 Steps to Improve Security of SCADA Networks" (2011); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_–_SCADA.pdf.

103 Amy Lee, John Vargo, Erica Seville: "Developing a Tool to Measure and Compare Organizations Resilience"; In: Nattural Hazards Review; ASCE, February (2013).

- на корпоративном/институциональном/личном уровне – система законов и правил эксплуатации; институциональные, региональные и культурные кодексы поведения; надлежащее образование; распространение информации и обучение для повышения уровня информированности в вопросах кибербезопасности;
- на глобальном уровне – следование всемирно признанным политическим соглашениям и – насколько это возможно – глобальным кодексам поведения; более конкретно, создание системы международных законов и правил эксплуатации, введение и соблюдение региональных и культурных кодексов поведения; введение надлежащего образования; распространение информационных материалов и обеспечение возможности профессиональной подготовки для повышения уровня информированности в вопросах кибербезопасности.

Вот далеко не полный перечень мер и методов повышения кибербезопасности и – как следствие – кибердоверия.

2.2 Повышение способности к восстановлению систем облачных вычислений и больших данных

Владимир Бритков

Основными новшествами в сфере ИКТ являются большие данные и облачные вычисления. По оценкам компании Gartner, 64% организаций во всем мире инвестируют или планируют инвестиции в большие данные. Под ними понимаются огромные объемы цифровой информации о людях и их окружении, которые, как ожидаются, будут удваиваться через каждые два года. Технологии больших данных включают новую область аналитики – "бизнес-аналитику", которая обеспечивает более высокую способность к восстановлению в киберсреде применительно к большим данным и облачным вычислениям.

Масштабные облачные инфраструктуры, большое количество и разнообразие источников и форматов данных, потоковый характер сбора данных и массовый переход между облаками – все это создает не имеющие аналогов уязвимости в области безопасности. Поэтому традиционных механизмов безопасности, которые рассчитаны на защиту небольших объемов статичных (в отличие от потоковых) данных, не достаточно. В этой статье рассматриваются десять основных задач, связанных с обеспечением безопасности и конфиденциальности больших данных, которые, как можно надеяться, привлекут повышенное внимание к укреплению инфраструктур больших данных.

Доверие – обязательное условие плодотворной деятельности, которое должно присутствовать в отношениях между поставщиком облачных услуг и клиентом, – является одним из наиболее значимых вопросов безопасности. Вместе с тем не существует каких-либо особых уз доверия, гарантирующих, что информация в облаке не станет объектом внутренней атаки или иного инцидента безопасности. Естественно, что компании учитывают этот важный фактор при участии в деловой деятельности с поставщиком облачных услуг. При этом клиенты могут заключить с поставщиком облачных услуг правовой договор на обслуживание (SLA), в котором указаны условия предусмотренных договором отношений между клиентом и поставщиком. Договоры SLA имеют особое значение для защиты клиентских данных, размещаемых при оказании облачной услуги, однако в связи с глобальным характером облака они обычно охватывают много юрисдикций, нередко имеющих различные применимые требования законодательства.

Инфраструктуры больших данных, как правило, официально являются проприетарными и изолированными от обычных сетей. В настоящее время большие данные в сочетании с внедрением технологий добычи данных легко доступны для больших и малых организаций по низким ценам с использованием облачных инфраструктур общего пользования. Инфраструктуры программного обеспечения позволяют разработчикам легко пользоваться тысячами вычислительных узлов для осуществления параллельных вычислений над данными. Для защиты инфраструктуры систем больших данных должна быть обеспечена защита распределенных вычислений и хранилищ данных. Для защиты самих данных при распространении информации должна сохраняться конфиденциальность, а чувствительные данные должны быть защищены с помощью криптографии и детального управления доступом.

Управление огромным объемом данных требует использования масштабируемых и распределенных решений как для защиты хранилищ данных, так и для обеспечения эффективных проверок и определения происхождения данных. Наконец, потоковые данные, появляющиеся из множества оконечных пунктов, должны проверяться на целостность и могут использоваться для проведения анализа инцидентов безопасности в реальном времени, чтобы обеспечить целостность инфраструктуры.

Десятью основными задачами, связанными с обеспечением безопасности и конфиденциальности данных, являются:

1. Защищенные вычисления в средах распределенного программирования.
2. Передовой опыт обеспечения безопасности нереляционных хранилищ данных.
3. Защищенные хранилища данных и журналы транзакций.
4. Проверка/фильтрация данных, вводимых в оконечном пункте.
5. Контроль безопасности в реальном времени.

6. Масштабируемые и компонуемые добыча и анализ данных с сохранением конфиденциальности.
7. Криптографически усиленная безопасность, ориентированная на данные
8. Детальное управление доступом
9. Детальные проверки
10. Происхождение данных

Обеспечение защищенной инфраструктуры больших данных

Для решения задач обеспечения безопасности и конфиденциальности, как правило, требуется рассмотреть три отдельных вопроса:

1. Моделирование: формализация модели угроз, которая охватывает большинство сценариев кибератак или утечки данных.
2. Анализ: нахождение поддающихся определению решений, основанных на этой модели угроз.
3. Реализация: реализация решения в существующих инфраструктурах.

Обеспечение защищенных вычислений в средах распределенного программирования

Сценарий использования: моделирование

Модель угроз для преобразователей включает три основных сценария:

1. Неправильное функционирование вычислительного рабочего узла – рабочие процессы, присвоенные преобразователю в облачной сети распределенных вычислений, неправильно функционируют из-за неправильной конфигурации или неисправного узла.
2. Атаки на инфраструктуру – на взломанных рабочих узлах может осуществляться перехват обмена данными между другими рабочими процессами и главным процессом с целью проведения атак повтором, атак через посредника и атак DoS на распределенные вычисления MapReduce.
3. Неавторизованные узлы данных – неавторизованные узлы данных могут быть добавлены в кластер, и в дальнейшем они могут получать дублированные данные или передавать измененный код MapReduce.

Анализ

С учетом изложенной выше модели угроз существуют два направления анализа: обеспечение благонадежности преобразователей и защита данных несмотря на наличие ненадежных преобразователей. Имеется два метода обеспечения

благонадежности преобразователей: установление доверия и обязательное управление доступом (MAC).

Реализация

MAC реализуется путем изменения структуры MapReduce, распределенной файловой системы и виртуальной машины Java с использованием SELinux в качестве базовой операционной системы.

Выводы

Большие данные заняли прочные позиции. Без них практически невозможно представить очередное приложение, потребляющее данные, создающее новые формы данных и содержащее алгоритмы, основанные на данных.

Вычислительная среда удешевляется, прикладная среда становится сетевой, а системная и аналитическая среда совместно используется через облако. В связи с этим возникают задачи по преодолению рисков, связанных с безопасностью, управлением доступом, сжатием, шифрованием и соблюдением, которые должны систематическим образом решаться. Эти задачи отражены в перечне из десяти основных проблем обеспечения безопасности и конфиденциальности, изложенных выше, которые должны быть решены, для того чтобы обработка больших данных и вычислительная инфраструктура стали более безопасными и способными к восстановлению.

Общие элементы, характерные для больших данных, обусловлены использованием для их обработки нескольких уровней инфраструктуры (как хранения, так и вычисления); использованием новых вычислительных инфраструктур, таких как базы данных NoSQL (для обеспечения высокой производительности, необходимой в связи с большими объемами данных), которые не были тщательно проверены на предмет безопасности; невозможностью масштабирования шифрования для больших наборов данных; невозможностью масштабирования методов контроля в реальном времени, которые могут подходить для меньших объемов данных; разнородностью устройств, которые создают данные; а также путаницей вокруг разнообразных правовых и политических ограничений, что приводит к использованию специальных подходов к обеспечению безопасности и конфиденциальности.

2.3 К системам управления, способным к восстановлению

Стефан Лудерс

Жизнь в сегодняшнем "вестернизированном" мире определяется системами управления, которые регламентируют практически все аспекты нашей повседневной деятельности. Мы живем в симбиозе[104] с системами управления и безвозвратно зависим от них. Без этих систем наше существование быстро уподобилось бы нормам жизни, существовавшим в средние века[105]. Учитывая нашу зависимость от систем управления, обеспечение их устойчивости и способности к восстановлению имеет жизненно важное значение.

Однако в наше время эти системы управления становятся уязвимыми вследствие отсутствия обеспечивающих их функционирование стандартных систем ИТ. Они используют те же инструменты, что и современные компьютерные центры: протокол Ethernet, TCP/IP, Всемирная паутина и электронная почта заменили связь на основе проприетарной полевой шины; ПК устранили потребность в неавтоматических дисплеях, датчиках и табло; операционная система Microsoft Windows вытеснила изготовлявшиеся на заказ терминалы с командной строкой.

Кроме того, высококачественное программное обеспечение – редкость и содержит дефекты, изъяны, недостатки и ошибки. В целях удовлетворения рыночного спроса программное обеспечение поставляется в форме бета-версий, в конце концов функционирующих, но обладающих изначальными недостатками и уязвимостями, которые обнаруживаются (и устраняются) позже. Пользователи и коммунальные предприятия необязательно требуют усовершенствований, учитывая связанные с этим расходы.

Ситуация осложняется тем, что стандартные ИТ открыли целый новый рынок для преступной деятельности – "темную паутину", где отдельные злоумышленники объединяют свои силы, для того чтобы проникать в системы ИТ и использовать их, подрывая доверия пользователей. В настоящее время каждая интерсеть, веб-сайт, операционная система и популярное программное приложение постоянно зондируются в поисках уязвимостей и слабых мест злонамеренными субъектами, стремящимися получить личную выгоду от их использования или продать их на черном рынке. А поскольку общая задача предупреждения таких атак или усиления

---

104 См. также публикации ЦЕРНа: Stefan Lüders "Our Life in Symbiosis" CERN Publications, 2014.

105 Это наглядно показано в романе-катастрофе Марка Элсберга – Marc Elsberg "Blackout: Morgen ist es zu spat" Blanvalet, March 2012.

способности к восстановлению после них многократно сложнее использования этих уязвимостей, злоумышленники получают выгоду от очевидного преимущества.

В целом ИТ до сих пор демонстрировали достаточную способность к восстановлению, которая позволяла избегать крупномасштабных последствий таких атак на нашу повседневную жизнь, и даже при том что "темная" экономика продолжает процветать, а международная правовая система пытается не отставать, население редко оказывается серьезно затронутым[106].

В результате экспоненциальных темпов развития систем управления и включения в них стандартных ИТ ситуация изменилась. Функциональные возможности ИТ идут на пользу этим системам, однако они сами обладают внутренними уязвимостями и недостатками. Это делает устойчивые, проприетарные и специализированные процессы управления хрупкими и незащищенными, и во все возрастающей степени анализируемыми злоумышленниками, что иллюстрируют следующие заголовки в СМИ: "Россия приветствует хакерские атаки" (The Register, 2000), "Хакеры наносят удар по системе водоснабжения Пенсильвании " (InTech, 2006), "Счетная палата США приходит к выводу, что электростанции TVA уязвимы для кибератак" (The Washington Post, 2008), "В хакерской атаке на систему водоканалов Калифорнии обвиняется инсайдер" (Computerworld, 2009), "ВВС США причинен "серьезный вред" в результате кибератак" (Flightglobal, 2009), "Проникновение шпионов в энергосистему США" (The Wall Street Journal, 2009), "Доклад: хакеры вторглись в системы управления воздушным движением ФАУ" (CNET, 2009), "Доклад: кибератаки вызвали отключение электроэнергии в Бразилии" (Wired, 2009), "Департамент внутренней безопасности: на службы водо- и энергоснабжения Америки ежедневно совершаются кибератаки" (Computerworld, 2012), "Защита шлюзов, насосных станций и мостов на низком уровне" (Radio Netherlands Worldwide, 2012), "Энергосистема США уязвима практически для всего" (OilPrice.com, 2012). Другая недавняя новость касалась диверсии на заводе по обогащению ядерного топлива в Натанзе, в Иране, о котором сообщили спецслужбы Израиля и США: "Вирус Stuxnet открывает новую эру в кибервойне" (Spiegel Online, 2010). Зараженные вирусом "Stuxnet" ПК на базе ОС Windows исказили изображения, предназначенные для операторов установок, осуществили загрузку в процессор системы управления и далее управляли скоростью вращения сотен центрифуг таким образом, что обогащение урана становилось неэффективным.

Событие с "Stuxnet" воспринимается как самая первая из документально подтвержденных кибердиверсий, однако оно отражает также дилемму финансируемых государствами кибератак. Ричард А. Кларк, бывший национальный

---

106 При возможном расширении атак на серверы доменных имен в международном масштабе, на основные маршруты интернета и, более широко, на частную жизнь граждан рядом государственных органов.

координатор правительства США по вопросам безопасности и борьбы с терроризмом заявил, что США могут взорвать ядерную установку или центр подготовки террористов в каком-либо месте, однако ряд стран могут нанести ответный удар, предприняв кибератаку, и "в отместку может быть разрушена вся экономическая система США [...] потому что в настоящее время мы не можем ее защитить".

В настоящее время действительно невозможно защитить системы управления теми же средствами, которые используются для защиты таких объектов, как компьютерный центр, например с помощью "внесения исправлений", то есть устраняя уязвимости путем обновления операционной системы.

Работу современных компьютерных центров направляют системы управления конфигурацией. Обновление и даже повторная установка больших групп серверов возможны, как правило, в короткие сроки. Этот процесс облегчают дублирование и виртуализация, поскольку профилактическое обслуживание происходит в подгруппах серверных пулов, а ядро продолжает обеспечивать операции. Гибкое "латание" систем управления, с другой стороны, в настоящее время ограничено редкими периодами обслуживания и строгим соблюдением требований, в частности для соответствующих процессов обеспечения безопасности. Безопасными считаются только те системы, которые полностью соответствуют требованиям и сертифицированы (например, повторная сертификация по уровню полноты безопасности, SIL). Полное тестирование, однако, требует времени и влечет дополнительные затраты. Кроме того, не всегда гарантируется полная совместимость новых исправлений операционной системы с существующим программным обеспечением систем управления, и продавцы, как правило, поздно объявляют о таком соответствии, если вообще объявляют. Усугубляют эту ситуацию встроенные системы, которые сложно модернизировать. Наконец, аппаратное оборудование компьютерных центров утилизируется каждые три - пять лет, однако в процессах управления старое оборудование используется возможно долго, даже значительно превышая заявленное время жизни операционной системы[107].

Другим примером служат разные подходы к контролю доступа. Услуги компьютерного центра отдают, как правило, приоритет конфиденциальности, целостности и доступности (то есть "КЦД"). Следовательно, контроль доступа имеет первоочередное значение, и методы аутентификации и авторизации являются полностью встроенными и централизованными и используют однократную регистрацию с использованием и без использования многофакторных проверок, управление сертификатами x509 и централизованные директории LDAP/AD. Системы управления отдают приоритет доступности по сравнению с конфиденциальностью и целостностью ("КЦД"). Следовательно, всегда должен гарантироваться доступ человека к процессу.

---

[107] Недавнее поэтапное снятие операционной системы Microsoft Windows XP создало еще одну серьезную проблему для коммунальных предприятий.

В целях упрощения передачи операций пароли используются операторами совместно. Кроме того, аппаратно-программные средства, которые зачастую являются проприетарными или устаревшими, поступают с неуказанными в документации путями обхода, работают с паролями по умолчанию, не позволяют блокировать неразрешенные соединения, используя внутренние брандмауэры или таблицы контроля доступа, и их сложно интегрировать в центральные решения управления определением идентичности. Шифрование рассматривается как требующий ресурсов процесс. Скорее, системы управления требуют или используют для поддержания своей безопасности и контроля доступа дополнительные защитные устройства. Значение надлежащей защиты сети постоянно возрастает, однако она не обеспечивается, так как парадигма хорошей "глубокоэшелонированной защиты" требует защитных средств на каждом уровне реального аппаратного оборудования, на котором работает операционная система и приложения.

Наконец, ключевое значение имеет устойчивость. Как упоминалось выше, стандартные системы ИТ в компьютерном центре, в особенности напрямую доступном из интернета, постоянно зондируются злоумышленниками на наличие дефектов. Центр может противостоять такому сканированию на возможность проникновения в систему и уязвимостей при условии надлежащего управления, поддержания уровня осведомленности по каждому аспекту этого явления и внедрения и мониторинга соответствующих систем обнаружения проникновения. Многолетний опыт и знания различных сценариев атак и потенциальных дефектов, а также принятые средства обмена информацией между заинтересованными сторонами облегчает защиту в случае инцидентов, их обнаружение и ответные действия. Системы управления, напротив, не могут рассматриваться как киберустойчивые. И если их аппаратная часть может быть устойчивой, их программная реализация неоднократно нарушала общие стандарты ИТ, не проходила базовые тесты на безопасность и не обладала основными средствами для их отражения[108]. Системы управления работают удовлетворительно в хорошо определенных сценариях использования, но не справляются, если сценарии использования определены менее точно. В отличие от стандартного аппаратного оборудования ИТ "безопасность" не является неотъемлемой частью устройств систем управления. Но даже если бы это было так, учитывая проприетарность и устаревание реализации безопасности, коммунальные предприятия сталкиваются с трудностями при выработке утверждения о том, действительно ли обеспечена надлежащая безопасность или это всего лишь мираж.

И наконец, сообщество систем управления стремится в настоящее время найти консенсус о том, как осуществлять "ответственное раскрытие информации", то есть как объявлять и публиковать вновь найденные уязвимости для соответствующего

---

108 "Проводимое в ЦЕРНе тестирование выявляет бреши безопасности в промышленных сетевых устройствах", *The Industrial Ethernet Book*, 2006.

поставщика и, позже, коммунальному сообществу. В мире стандартных ИТ срок от трех до девяти месяцев между уведомлением поставщика программного обеспечения и полного раскрытия этой информации общественности считается приемлемым, но некоторые полагают, что это слишком короткий период, учитывая что жизненный цикл разработки программного обеспечения для программного управления занимает значительно больше времени и что применение исправлений на коммунальном предприятии должно четко координироваться и осуществляться по графику. На практике весь этот процесс длится, как правило, около года.

Эта проблема должна быть преодолена, если системы управления будут обладать способность к восстановлению в киберсреде. Системы управления должна обеспечивать превращение безопасности в неотъемлемую часть общей функциональности, доступности, используемости, эксплуатационной технологичности и защищенности. Эксперты по системам управления должны участвовать в проведении соответствующей подготовки в области ИТ и, в частности, безопасности ИТ. Подготовка должна начинаться на образовательном уровне в колледжах и университетах, где безопасность следует включать в учебные программы, а не рассматривать этот предмет как "дополнительный". Или, что еще лучше, все связанные с ИТ задачи следует передать на внешнее исполнение компетентным специалистам в области ИТ, которые могут провести разницу между соответствующими потребностями, связанными с эксплуатацией систем управления и компьютерных центров. Могут потребоваться новые компромиссные решения, для того чтобы заново уравновесить потребность в постоянной доступности и оперативном внесении исправлений, в простом доступе и жестком контроле доступа. Наряду с этим методы виртуализации ИТ могут стать панацеей, необходимой для преодоления этих проблем, и служить новой основой для развертывания введения исправлений с разбивкой на этапы тестирования, предпроизводственного процесса и операционных систем. Стандартом для систем управления должны также стать полное управление разработкой программного обеспечения, системы управления версиями, 360° жизненные циклы разработки программного обеспечения, тщательное регрессивное тестирование и ночные сборки. Еще одним обязательным требованием является проведение детально документируемых и постоянно обновляемых инвентаризаций. Тщательное документальное оформление базы установки, всех устройств, учетных записей, приложений, включая их взаимозависимость, является обязательным для понимания рисков и использования защитных мер. Тестирование на возможность проникновения в систему должно стать операцией по умолчанию. В идеальном случае общепринятые и полностью открытые наборы правил и процедуры для проведения оценок уязвимости становятся стандартом, так чтобы поставщики и производители, коммунальные предприятия и интеграторы, но также и правительства, академические организации и органы по сертификации могли независимо оценивать безопасность данных устройств, аппаратных и программных средств управления. Эти процедуры обязательно повысят устойчивость современных систем управления, усилят с

течением времени их способность к восстановлению после злонамеренных действий и, возможно, проложат путь к схеме сертификации, подобной ISO9001.

Все эти шаги не являются ни тривиальными, ни удобными. Для современного поколения систем управления и экспертов в области систем управления это может быть даже слишком поздно. Таким образом, мы должны сосредоточиться на будущем и нацелиться на еще большем объединении ИТ систем управления и компьютерных центров. Степень достигнутого нами успеха станет оселком при определении облика нашего будущего.

2.4 Способность к восстановлению в киберсреде с позиций частного сектора

Данил Кермини

Мы живем в невероятно сложном и гиперсоединенном мире. Этот мир создает беспрецедентные возможности и риски, невообразимые еще несколько лет назад. Мы только сейчас начинаем понимать социальные, политические и экономические изменения, которые он обусловливает, приспосабливая нормы, политику и бизнес-модели к метафизике сети.

Все эти изменения заново определили способы взаимосвязи физических лиц, предприятий и правительственных органов. Традиционные методы создания и потребления экономической ценности подвергаются воздействию со стороны новых бизнес-моделей и новых видов социального взаимодействия, обусловливаемых гиперсоединенностью. Уже сейчас отрасли все шире используют цифровые каналы для своих внутренних операций, а также взаимодействия со своими партнерами. Структуры, которые никогда не рассматривались как ключевые игроки в области технологий, занимаются теперь вопросами, лежащими за пределами области их компетенции и комфорта.

Потребители все более стремятся к расширению своих прав и возможностей, получению более полных информационных потоков и богатству выбора. Компании изучают поведение потребителей как никогда глубоко, предоставляя им беспрецедентные возможности индивидуализации. Они также ставят задачу адаптации к быстро меняющейся среде, с тем чтобы отвечать новым ожиданиям потребителей, таким как совместное создание и оперативная разработка прототипов.

Гиперсоединенность становится катализатором, снижающим препятствия для выхода на рынок, содействующим торговле и активизирующим конкуренцию внутри и между секторами, постоянно переопределяя отраслевую картину, а также нарушая политическую изолированность. Непрерывная автоматизация различных задач и

процессов – часть более широкого движения к экономикам знаний – создает существенную нагрузку для традиционных рынков труда.

Темпы инноваций достигли этапа, когда не только ликвидируются рабочие места производственных рабочих, но и экспертные профессии претерпевают долговременные структурные сокращения. Наряду с этим наша образовательная система не способна отвечать потребностям людей в приобретении новых специальностей (например, специалисты в области данных), вытесняющих более традиционные занятия.

Движущими силами этих преобразующих перемен являются информационно-коммуникационные технологии. Гиперсоединенность создается технологическими компаниями во всем мире и является критерием любого определения технологической компании. Услышав разговор руководителей автомобильной отрасли о машинах, можно подумать, что речь идет о терминалах на колесах. Медицинские компании говорят о данных, а банки – о кибербезопасности. От банковской сферы и потребителей до компаний энергетической отрасли, все во всем мире – в первую очередь мыслят в цифровых категориях.

Если в прошлом технологические компании выступали разрушителями различных бизнес-моделей и преобразующей силой в других отраслях, в современной ситуации другие отрасли становятся разрушителями ранее сформировавшихся цифровых бизнес-моделей.

Этот сдвиг отражается и в нашем коллективном сознании потребителей. По данным недавнего доклада Interbrand[109], восемь из десяти ведущих брендов принадлежат компаниями ИКТ. Половина брендов в следующей десятке – бренды, известные в каждом доме, с помощью которых мы формируем современный технологический ландшафт. Общая стоимость этих чисто технологических брендов первой двадцатки составляет более триллиона долларов. Если бы это была одна страна, она вполне заняла бы место в Группе двадцати (G20).

В 2014 году тремя ведущими котируемыми компаниями по рыночной капитализации стали также компании ИКТ. В последнем составленном журналом Fortune списке наиболее влиятельных людей шесть из первых двадцати являются представителями технологического сектора; одиннадцать – политические и религиозные лидеры; остальные три места занимают CEO из финансового сектора, сферы розничной торговли и энергетической отрасли[110]. Интересно, как распределятся места в списке 2015 года.

---

109 http://www.interbrand.com/en/best-global-brands/2013/Best-Global-Brands-2013.aspx

110 http://www.forbes.com/powerful-people/list/

Усиливается сформировавшаяся опора на киберпространство в нашей ежедневной деятельности. Следствием этого является наша обеспокоенность рисками, которые оно несет, а также страх, что оно станет недоступным. Незнакомое всего несколько лет назад понятие "способность к восстановлению в киберсреде" теперь стало во всем мире постоянной темой обсуждений на крупных встречах, политических дискуссиях, а также в разговорах в барах и дома. Мир узнает, что все, что подключено, может быть взломано, и что невозможно быть постоянно полностью защищенным, скорее можно быть гибким и способным к восстановлению, для того чтобы обеспечить функционирование в неблагоприятных условиях.

Скорость, мобильность и сотрудничество – ключевые характеристики успешного предприятия в цифровую эпоху. Для того чтобы и далее использовать преимущества гиперсоединенности, срочно необходима международная экосистема, обладающая способностью к восстановлению в киберсреде. В последние два года Всемирный экономический форум собирает группу руководителей и ответственных за выработку политики лиц, для того чтобы изучить путь к созданию более устойчивой к кибервоздействию цифровой среды. Общим знаменателем для различных министерств и отраслей является обеспокоенность резким увеличением числа киберинцидентов в мире. Заимствуя концепцию из экологического права, можно сказать, что признаются общие, но дифференцированные обязанности заинтересованных сторон, когда это касается киберпространства, но способность к восстановлению в киберсреде требует высокой степени взаимодействия многих заинтересованных сторон. Как и в других областях глобального управления, развивающиеся страны, в которых зачастую отсутствует детальное понимание киберугроз и потенциал для надлежащего реагирования на них, оказываются затронутыми новой совокупностью рисков аналогично развитым странам. Очевидно, что по мере усиления зависимости наших экономик от цифрового соединения, способность к восстановлению в киберсреде становится для руководителей всех отраслей и политических направлений ключевой сферой компетенции.

В ответ на эту обеспокоенность Всемирный экономический форум разработает тему способности к восстановлению в киберсреде, предлагая главным исполнительным директорам (в противоположность главным директорам по информационной безопасности, главным директорам по технологиям и т. д.) и государственным должностным лицам высоко ранга признать взаимозависимость всех сторон, играющих роль в содействии формированию способного к восстановлению общего цифрового пространства. Проводя эту деятельность, мы подчеркиваем роль лидеров, поощряя обеспечение осведомленности и комплексное управления рисками. Мы настоятельно рекомендуем также принимать многосторонний системный подход к обеспечению способности к восстановлению в киберсреде, так как деятельность предприятия не ограничивается пределами его корпоративной среды, а распространяется на всю цепочку создания ценности – от поставщика до потребителя.

Значение способности к восстановлению в киберсреде убедительно подтверждается цифрами наряду с отношением общественности. В ближайшие годы ежегодные расходы на обеспечение способности к восстановлению в киберсреде вероятно возрастут с 69 млрд. долл. США в 2013 году до 123 млрд. долл. США в 2020 году[111]. Эти оценки безусловно зависят от рыночного анализа, который, в свою очередь, будет учитывать существующие и прогнозируемые киберугрозы. Таким образом, по одному сценарию инвестиции в способность к восстановлению в киберсреде возрастают на 13% до 139 млрд. долл. США в год в результате укрепления сотрудничества государственного и частного секторов, которое отражает их оборонительный потенциал. По другому сценарию можно ожидать увеличения расходов на 28%, т. е. 157 млрд. долл. США в год, если наступательный потенциал и разобщенные ответные меры перевесят оборонительный и коллективный потенциал.

Обсуждение киберрисков все чаще сводится к сценариям светопреставления или грозного "кибергеддона" и изобилует ставшими расхожими выражениями "конфиденциальности более не существует" или "слабое звено". Однако не меньшую обеспокоенность должны, вероятно, вызывать утраченные возможности вследствие существенного движения назад или фрагментации существующей цифровой экосистемы. Обратный ход может возникнуть в результате одного крупного "кибергеддона" или постепенного разрушения ("не мытьем, так катаньем").

Фрагментация может происходить на региональном, национальном уровне и уровне предприятия, и может существовать большое число причин, в силу которых многочисленные участники выбрали именно такой образ действий. Следовательно, фрагментация могла начаться, поскольку правительства, обеспокоенные отсутствием вызывающей доверие среды, призваны выполнять свои функции по обеспечению безопасности в киберпространстве. Фрагментация может также начаться как следствие фрагментации отраслевой политики и регулирования в различных юрисдикциях.

По оценкам Mckinsey, если возрастающая изощренность атак приведет к снижению инвестиций, мировая экономика может потерять 3 трлн. долл. США потенциального экономического роста[112]. Сложная политическая картина может еще более усложнить процесс принятия экономических решений.

Итак, что же означает способность к восстановлению в киберсреде с позиции предприятия? Она начинается с признания взаимозависимости, подхода на основе оценки рисков, предусматривающего лишь частичное смягчение последствий рисков в качестве основополагающей характеристики любой сложной системы, и

111 http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

112 Там же.

предположения, что способность к восстановлению одной организации способствует обеспечению способности к восстановлению всей системы.

Компании, как и другие организации, придают огромное значение приоритетам руководства. Следовательно, важно привлекать их команды высшего руководства и обеспечивать структуры управления для надзора, такие как комитеты, для разработки эффективной программы управления киберрисками и контроля за ее выполнением.

Комплекс дифференцированных обязанностей и общих задач должна обеспечивать команда руководства, которая поддерживается ресурсами, управлением, обязательствами и наглядностью этих усилий. В аспекте обеспечения устойчивости функционирования предприятия большую пользу может принести стресс-тестирование и "военные учения" с проигрыванием потенциальных кризисных сценариев, которые требуют координации участия различных подразделений – от ИТ до связей с общественностью, так как если возникнет реальная ситуация, не останется времени для продумывания участниками своих обязанностей и возможных ответных действий.

Также полезной может стать полностью интегрированная способность к восстановлению в киберсреде в качестве стандартного компонента более широкого бизнес-сообщества и управления рисками предприятия. Хорошей отправной точкой может стать определение информационных активов, имеющих критическое значение для деятельности предприятия. Оборона по периметру могла бы быть хорошей стратегией в прошлом, но при современном уровне атак, зондировании и внутренних угроз сложившаяся структура рисков требует четкой приоритезации активов, что позволит направлять достаточные ресурсы для их защиты.

Это означает, что все аспекты операций, а также репутационный риск должны стать предметом периодических оценок воздействия. Следует также ввести процессы, необходимые для сокращения времени реагирования, с тем чтобы обеспечить возможность полного или частичного восстановления в случаях крупных отказов. Очень важно, чтобы это выполнялось в рамках всей компании и не рассматривалось как вопрос, которым должно заниматься исключительно подразделение ИТ.

Все подразделения, включая подразделения маркетинга, по связям с государственными органами и общественностью и привлечению потребителей, возглавляемые командой высшего руководства, должны быть готовы к одновременному решению задач восстановления затронутых операций, смягчения последствий вероятного негативного воздействия на бренд и оттока клиентов, а также к возможным регуляторным последствиям.

Многие успешные компании создали у себя головной офис по информационной безопасности. В некоторых компаниях эта функция полностью отделена от обязанностей главного директора по технологиям/главного директора по информационным технологиям. Кроме того, в ряде компаний обеспечивается, что

даже при разном ранге этих постов порядок их подчиненности дифференцируется как стратегические задачи разных функций, которые могут потребовать разных приоритетов по таким вопросам, как например техническая архитектура и приобретение.

Только путем разработки всеобъемлющего обзора различных информационных активов, а также значимости адекватного своевременного реагирования на потенциальное нарушение в рамках организации компания может реально способствовать обеспечению собственной системной способности к восстановлению в киберсреде. При внедрении компаниями структур обеспечения способности к восстановлению в киберсреде/управления рисками одним из важных элементов, который необходимо учитывать, является соответствие, поскольку правительства начинают решение проблемы снижающегося уровня безопасности с помощью различных регуляторных механизмов, от добровольных кодексов поведения и передового опыта до обязательного сообщения об инцидентах и введения стандартов.

Еще одним важным фактором является роль поставщиков, подрядчиков и потребителей во всей киберцепочке поставок. Предприятие должно стремиться к улучшению во всей широкой экосистеме, увеличивая таким образом периметр безопасности и обеспечивая процесс создания коалиции.

Одно из важнейших направлений международного бизнеса в последние годы составляет проактивная оборона. С ростом сложности определения периметра безопасности успешные предприятия будут использовать существующие внутренние и внешние информационные точки, для того чтобы получать сведения об изменениях в структуре угроз, которые могут привести к атаке. Однако существует значительный разрыв в понимании того, в какой точке уровень угроз пересекает порог внутренне-внешнее, не говоря о возможности превентивного действия и вопроса его законности даже в условиях явной и требующей мер опасности.

Трудности отнесения приводится зачастую в качестве одного из основных препятствий, но таким же препятствием являются правомерность и законность потенциального действия. Эта неопределенность начинает немного проясняться в тех случаях, когда существует всесторонняя киберстратегия на национальном уровне и на уровне предприятия, что не всегда легко достижимо. Такая стратегия должна содержать ясные и прозрачные внутренние, а также международные компоненты.

В руководстве компаний произошел существенный сдвиг от признания этой проблемы к более детальному пониманию компонентов и возможных методов смягчения последствий. По мере дальнейшего быстрого изменения структуры угроз на национальном и международном уровнях формируется диалог с участием многих заинтересованных сторон.

Гиперсоединенность уже изменила способы нашего общения: она воздействует на наши процессы принятия решений и по-новому организует нашу жизнь.

Разрушительное воздействие информационно-коммуникационных технологий все чаще обусловливает социально-экономические преобразования. Мы склонны переоценивать краткосрочное воздействие технологий и недооценивать их долгосрочное воздействие на все аспекты нашей жизни. Концепция способности к восстановлению в киберсреде может стать отправной точкой для понимания и выработки схем, которые будут направлять процесс принятия решений для достижения тех результатов, которых мы все желаем.

2.5 Континуум кибербезопасности для укрепления способности к восстановлению в киберсреде

Соланж Гренаути

Разные измерения способности к восстановлению в киберсреде

Киберриски представляют реальную угрозу для каждого. Убедить в этом может обычный просмотр новостей. Киберпреступность стала всемирным бедствием, а кибератаки – частью военных доктрин. Состоявшийся в сентябре 2014 года саммит НАТО[113] определил массовые кибератаки как военные действия, которые могут повлечь за собой ответные военные действия, и если объектом атаки станет какой-либо член НАТО, то это будет рассматриваться как нападение на НАТО в целом. Необходимо признать, что конфликты разворачиваются также и в киберпространстве, как правило, в форме кибератак, нацеленных на объекты гражданской и военной инфраструктуры, а также в форме манипулирования информацией. В интернете маркетинг войны и терроризма идет бок о бок с маркетингом законного и незаконного бизнеса, в то время как киберпреступный черный рынок процветает. Интернет также становится популярной средой связи для преступной деятельности и пропаганды. Атаки на информационные системы могут прервать функционирование важнейшей инфраструктуры страны, реализовать стратегии преступления, вызвать утрату производительности и конкурентоспособности или способствовать захвату власти в стране. Наряду с этим интернет упрощает деятельность, направленную на замедление или сдерживание экономического развития страны, нарушение нормального функционирования государства или его дестабилизацию. Огромное число информационных систем являются мишенями кибердеятельности, цель которой заключается в дестабилизации страны путем нанесения ущерба ее экономике, институтам и репутации. Такая деятельность совершается в широком контексте глобальной экономической гиперконкурентности.

---

113 http://www.nato.int/cps/en/natohq/news_112107.htm?selectedLocale=en (NATO Wales Summit Guide − Newport, 4−5 September 2014).

Многофакторные киберугрозы постоянно эволюционируют и важно понимать их в междисциплинарном и глобальном аспекте, для того чтобы постоянно противостоять им, укреплять безопасность и способность к восстановлению объектов гражданской и военной инфраструктуры, а также защищать всех участников экономической деятельности, включая малые и средние предприятия и физических лиц. Постоянный процесс поддержания кибербезопасности физических лиц и имущества, а также обеспечения общественной безопасности должен стать частью политического проекта, поддерживающего стратегию долговременного развития для общества, в котором учитываются его культурные и другие особенности. Это требует участия всех субъектов – государственных и частных – как на национальном, так и на международном уровнях[114].

Мы создаем мир постоянной соединенности на основе подвижной, беспроводной и бесконтактной[115] связи, мир, в котором объекты становятся интеллектуальными и способными общаться: это интернет вещей и практически всего, что содействует развитию "умных" домов и городов. Обычные объекты, например автомобили и светофоры, будут включать компоненты ИТ и интернет-технологии. Таким образом, благодаря встроенным в их программную часть средствам интеллектуального управления, они приобретут определенную автономность и способность принятия решений. Уже начинается размещение в общественных зонах таких объектов, и они автоматически становятся потенциальными мишенями злонамеренной кибердеятельности, так как любой объект, подключенный к интернету, может быть взломан и превращен в часть ботнета для совершения атак на другие системы. Низкий уровень безопасности таких объектов может иметь разрушительные последствия для нашей физической безопасности. Что касается помощи людям и повседневной деятельности, то в нашу жизнь постепенно входят роботы разного уровня сложности. Такие роботы могут воздействовать на наше поведение и окружающую нас среду, поэтому контроль над ними со стороны злонамеренных или нежелательных объектов может также иметь негативные последствия для нашего общества. Двадцать первый век – это век электронных чипов RFID и нанотехнологий – идея интеллектуальной пыли. Конвергенция электронного и биологического миров постепенно приобретает черты реальности, в частности в отношении человеческого тела и различных датчиков, протезов и других элементов биомедицинской электроники, которые могут быть имплантированы в человеческое тело для устранения каких-либо его дисфункций (например, инсулиновые помпы и кардиостимуляторы). Уже существующие нейронные интерфейсы позволяют взаимодействовать с компьютерами силой мысли. И если все это может способствовать благополучию по мере все большей многогранности их использования и конвергенции электронного и биологического

---

114 "Cyberpower: crime, conflict and security in cyberspace"; S. Ghernaouti, EPFL Press 2013.

115 Бесконтактная связь относится к технологиям связи в ближнем поле (NFC).

миров, то захват их исходного назначения может привести к случаям взлома, включая человеческую мысль. Эти новые риски заставляют нас заново переосмысливать безопасность, для того чтобы совершенствовать управление такими объектами и сохранять наши ценности, подвергающиеся опасности в результате возрастающего воздействия технологий на общество.

Киберпространство становится элементом цивилизации, на который мы в значительной степени полагаемся. Значит, важным становится, чтобы его инфраструктура была устойчивой и способной к восстановлению после инцидентов любого вида. Концепция способности к восстановлению в киберсреде охватывает несколько измерений, которые можно разделить на оперативные меры, такие как борьба против киберпреступности, взаимодополняемость мероприятий, связанных с кибербезопасностью и киберзащитой, эффективное управление рисками, касающимися энергетики и экологии, а также образование и поддержание уровня знаний людей, необходимого для будущего информационного общества.

Борьба с киберпреступностью

Все большую обеспокоенность международного сообщества вызывает проблема повышения уровня готовности к борьбе с киберпреступностью. Ни одно государство, ни одна организация и ни один пользователь интернета не огражден от кибервредоносности преступного или ирритативного происхождения.

Более высокий уровень подготовленности к борьбе с киберпреступностью предполагает наличие некоего низкого или недостаточного уровня готовности. Для учреждений это может иметь следующую форму:

- наличие средств (т. е. стратегии, меры, ресурсы, квалификация), необходимых для решения проблемы, количественный или качественный уровень которых, однако, недостаточен;
- наличие средств защиты, эффективность и пригодность которых не соответствуют требуемому уровню.

При том что эти две ситуации весьма распространены, необходимо все же заметить, что для многих субъектов, таких как малые и средние предприятия и физические лица, а также для многих объектов инфраструктуры и подключенных к интернету объектов не имеется внедренных структур управления или мер безопасности.

Для государства основу борьбы с киберпреступностью составляет ряд предпосылок:

- существование нормативно-правовой базы, применимой на национальном уровне, которая совместима с международными структурами;
- наличие судебных структур и полицейских сил, обладающих соответствующими ресурсами и квалификацией для работы на национальном

уровне и сотрудничества с международной сетью в целях борьбы с транснациональной киберпреступностью.

На международном уровне это предполагает, что международное сообщество объединится вокруг общего дела борьбы с киберпреступностью и что не существует благоприятной среды для создания цифрового рая, откуда мошенник может действовать абсолютно безнаказанно.

Такая ситуация была бы на пользу преступникам, которые:

- рассматривают интернет как среду совершения экономических преступлений и как инструмент осуществления преступных деяний (торговля людьми, незаконный оборот наркотиков, отмывание денег…);
- рассматривают киберпространство как защитный уровень и глобальное игровое поле.

Борьба с преступностью всегда была сложным делом. Киберпреступность еще более его усложнила и усилила трудности борьбы с преступностью, будь то на национальном или международном уровне.

В то же время о деяниях киберпреступников регулярно сообщается в СМИ, но они не сопровождаются, как представляется, достаточно эффективными мерами, направленными на ограничение роста мощи киберпреступников или сокращению числа жертв; по-прежнему мало арестов и судов в сравнении с масштабами распространения злонамеренной деятельности, и это приводит к тому, что чувство справедливости пострадавших не удовлетворяется в полной мере.

Несмотря на это, действия государств по борьбе с киберпреступностью увенчались двумя крупными достижениям:

- на европейском уровне – создание в 2013 году в рамках Европола Европейского центра по борьбе с киберпреступностью (EC3) в Гааге[116];
- на международном уровне – открытие в 2014 году в Сингапуре Глобального инновационного комплекса Интерпола[117].

Эффективная борьба с киберпреступностью требует упреждающего подхода, который делает киберпространство менее привлекательной средой для киберпреступности и сужает возможности для преступной деятельности. Следовательно, необходимо усложнять осуществление кибератак, повышая таким образом их стоимость в аспекте компетенции и ресурсов и, следовательно, снижая ожидаемые выгоды и увеличивая риски для преступников быть опознанными, обнаруженными и привлеченными к

116 https://www.europol.europa.eu/ec3

117 http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation

уголовной ответственности. В целом повышение способности к восстановлению можно достичь с помощью следующих мер:

- сокращение числа технических, организационных, правовых и человеческих уязвимостей;
- усиление устойчивости и способности к восстановлению информационной инфраструктуры, применяя согласованные и дополняющие друг друга технологические, процедурные и управленческие меры;
- создание реального потенциала для адаптации мер обеспечения кибербезопасности и киберзащиты к постоянно развивающейся ситуации;
- наличие мер по управлению киберкризисами;
- борьба со схемами монетизации киберпреступности.

Новое поле киберпространства заполнено всеми видами деятельности. Это инструмент на службе экономической эффективности и место, где можно проявлять силу: это, по существу, стратегическая территория. Следовательно, ее необходимо защищать и охранять в категориях экономической и национальной безопасности.

Гарантия континуума защиты безопасности для обеспечения определенного уровня стабильности

Управление киберрисками осуществляется в условия безжалостной и постоянной экономической конкуренции (практически экономической войны), поиска немедленной прибыли, международного валютного кризиса, общего беспорядка, социальной несправедливости, экологического кризиса и определенного дефицита глобального управления. Кибербезопасность не должна рассматриваться изолировано в контексте логики ответных мер, направленных на "выживание" после киберинцидента – намеренного или случайного. При том что способность противостоять является основополагающей и абсолютно необходима, она не может стать заменой глобального подхода с участием многих сторон как на национальном, так и на международном уровнях или реального понимания всего явления киберпреступности и киберконфликта. Глобальный, междисциплинарный и комплексный подход к обеспечению кибербезопасности и киберзащите позволит принимать и упреждающие и ответные меры, эффективность которых будет зависеть от того, насколько они всесторонни и согласованы с гражданской и военной точек зрения. Утопией было бы предполагать, что мы сможем реагировать на киберпроблемы в отсутствие многоуровневого сотрудничества между многими сторонами внутри и за пределами национальных границ, направленного на обеспечение стратегий поддержания мира в киберпространстве и в физическом мире.

В некоторых случаях может быть необходимо заново осмыслить сотрудничество между гражданскими и военными организациями и диалог между ними, с тем чтобы обеспечить согласованный континуум защиты безопасности для общества в целом.

Кибербезопасность можно понять, только применяя трансдисциплинарный и обобщающий подход. На национальном уровне это означает совместное и сквозное видение проблемы, укрепление межведомственного сотрудничества и способность к совместной работе.

Какова бы ни была основная цель кибератаки, что бы ни было ее объектом (отдельное лицо, организация, государство), применяемые инструменты одинаковы. Природа и масштаб воздействия различен в зависимости от объекта и намерений нападающих, но используемые методы и инструменты остаются теми же. Когда речь идет о какой-либо стране, обеспечение общественной безопасности, экономической безопасности и национальной безопасности – все это относится к континууму гражданской и военной безопасности. Поэтому столь важно, чтобы это было закреплено в национальных стратегиях кибербезопасности и киберзащиты, для оптимизации эффективности и действенности принимаемых мер, также для реагирования наилучшим образом на потребности населения, как в мирное, так и в военное время. Тем не менее защита важнейшей инфраструктуры не может быть вопросом, который частный или государственный сектор решают в одиночку, – элемент, который также обосновывает необходимость континуума защиты безопасности.

Важно защищать и оборонять как цифровые активы, так и наследие частных лиц, организаций и государств, а также инфраструктуры, которые поддерживают как эти активы, так и имеющие решающее значение функции. Для этого требуются дополнительные меры защиты, включая виды деятельности, соответствующие как гражданскому, так и военному пониманию понятия "защита", направленные на обеспечение безопасности инфраструктур и активов, уязвимых в отношении киберугроз.

Создание культуры кибербезопасности и киберзащиты при поощрении международного диалога по этим вопросам должно способствовать, в нашем сложном и неопределенном мире, определенному уровню доверия и стабильности, при условии что все заинтересованные стороны ведут себя честно и несут коллективную ответственность. Следует принимать во внимание необходимость управлять энергетическими и экологическими рисками.

В числе косвенных рисков, создаваемых цифровыми обществами и масштабными видами использования информационных систем, которые оказывают огромное влияние на нашу планету, не следует забывать, в долгосрочной перспективе способности к восстановлению в киберсреде, о разработке мер, которые обеспечат нам устойчивость в плане наличия энергии и сохранения природных ресурсов и экологической среды для будущих поколений.

Вследствие этого мы должны в первую очередь уделять внимание рискам, связанным с:

- удалением и утилизацией электронных отходов;

- потреблением энергии (растущими и постоянными потребностями в электроэнергии);
- климатическим потеплением (выбросами тепла и необходимостью охлаждать компьютеры и парки серверов);
- эксплуатацией редкоземельных элементов и металлов, необходимых для производства электронного оборудования;
- экологическими последствиями кибератак против систем, управляющих очистными сооружениями, производством и распределением токсичных продуктов, систем пожарной тревожной сигнализации и т. п.

Деятельность по обеспечению способности к восстановлению в киберсреде должна также соответствовать требованиям к защите важнейшей инфраструктуры, в первую очередь основных элементов, связанных с энергией и окружающей средой.

Применение упреждающего подхода для более эффективного предвидения угроз, управления киберрисками, обнаружения аномалий для ограничений их последствий и развития способности к восстановлению в киберсреде в экологическом плане является коллективной ответственностью. Необходимо гарантировать образование и создание человеческого потенциала.

Теории и постулаты в отношении кибербезопасности предполагают наличие людей, прошедших подготовку в области кибербезопасности по нескольким дисциплинам из числа социальных или технических наук; то есть предполагается, что такие образовательные возможности существуют. Без наличия во всем мире навыков и квалификации в области кибербезопасности и без передачи знаний и сотрудничества для создания человеческого потенциала будет сложно разработать стили поведения, совместимые с кибердоверием. Надлежащая практика в области ИТ и осознание киберрисков важны, но недостаточны, если концепция кибербезопасности не интегрируется в товары и услуги уже в начале этапа проектирования; или если системы полиции и правосудия не в состоянии выполнять свои функции из-за отсутствия квалификации; или если политические и экономические субъекты, как все интернет-пользователи, от самых молодых до самых старых, не обладают необходимыми навыками, знаниями и опытом. Недостаточно проинформировать население о существующих в интернете опасностях и об элементарных мерах предосторожности, которые необходимо принимать, или возлагать только на граждан ответственность за ситуации, которые они в большинстве случаев не в состоянии контролировать. На практике было бы несправедливо, чтобы конечные пользователи и граждане несли расходы, связанные с рисками, не возлагаемые на тех, кто их создал, тем самым перекладывая проблему общества на людей, которые сами не располагают необходимыми для ее решения знаниями и средствами.

Способность к восстановлению в киберсреде как новая задача в рамках кибербезопасности

Способность к восстановлению после преступных событий представляет собой часть глобальной концепции кибербезопасности и способствует выработке кибердоверия. Сегодня существует насущная необходимость укрепить прочность наших инфраструктур и их способность к восстановлению посредством надлежащих технических, правовых, организационных и процедурных мер. Как и все виды деятельности в сфере безопасности, борьба с киберпреступностью, злоупотреблениями в киберсреде и ненадлежащим применением киберсредств носит сложный характер. Эту борьбу следует вести с учетом защиты людей и материальных и нематериальных активов и охраны общих, повсеместно принятых демократических ценностей. Ввиду этого полезно иметь эффективный и действенный подход к кибербезопасности и способности к восстановлению в киберсреде.

Чтобы в информационном обществе не воцарились недоверие и слежка, необходимо найти убедительные ответы на проблему необходимости создания доверия и способности к восстановлению в киберпространстве, а также выработать практические варианты защиты цифровых активов и инфраструктур. Любая попытка ограничить нисходящую спираль киберпространства в этом отношении потребует политической воли на национальном и международном уровнях, ресурсов и навыков, организационных структур и процедур, а также налаженной координации. О каких бы субъектах ни шла речь – законных или вызывающих сомнения – новый фактор стабильности обществ составляет часть их безопасности и связан с их способностью контролировать киберриски и удерживать кибернеприятности на приемлемом уровне. Кибербезопасность должна быть не инструментом главенствования и проявления мощи государств, а инструментом стабильности и миротворчества[118].

Глава III: Киберсвобода

Введение

В предыдущей главе подчеркивалось решающее значение создания способности к восстановлению в киберсреде, чтобы обеспечить наличие киберпространства, внушающего доверие, а в этой заключительной главе представлен обзор проблем киберсвободы и возникающих в связи с ней угроз как в государственном, так и в частном секторе, которые подрывают надежду достичь свободы в интернете.

---

[118] Обеспечение кибердоверия на глобальном уровне будет способствовать решению основных вопросов кибермира, таких как поднятые в публикации "В поисках кибермира" – МСЭ, 2011 год (http://www.itu.int/pub/S-GEN-WFS.01-1-2011).

Свобода выражения мнений и свобода слова, свободный доступ к информации и право на конфиденциальность всегда были основными элементами гражданского общества, поскольку они отражают основополагающие права человека и гражданские свободы, которые лежат в основе демократических принципов и ценностей. Появление интернета и информационно-коммуникационных технологий дало миллиардам людей во всем мире возможность получить доступ к непредставимым до тех пор объемам информации и средствам связи. Они фактически представляют собой гигантские платформы для обмена мнениями, данными и инновационными идеями. Но в то же время эти важнейшие инструменты цифрового века также используются для подрыва прогресса, политических прав и конфиденциальности, тем самым разрушая доверие к их применению.

Как не раз отмечал Европейский суд по правам человека: "Свобода выражения мнений [...] применима не только к "информации" или "идеям", которые воспринимаются положительно или считаются неоскорбительными или нейтральными, но и к тем, которые оскорбляют, шокируют или беспокоят государство или какой-либо сектор населения"[119].

Хотя блоги и социальные сети открывают новые перспективы обмена идеями, в последние годы некоторые государства прибегают к блокированию интернета в качестве дальнейшего распространения государственной цензуры, направленной на управление общественным мнением и подрыв свободы информации и выражения мнений.

Это создает угрозу для привлекательных черт интернета, к которым относятся его безграничная повсеместная распространенность и доступность во всем мире, вызывая ведущееся в настоящее время обсуждение сетевого нейтралитета, в котором основное внимание уделяется проблеме гарантирования равных прав доступа к этому важнейшему средству общения нашего времени.

Современное информационное общество характеризуется огромным объемом легко доступной информации, что увеличивает значение возникающих угроз шпионажа как в государственном, так и в частном секторе, ставя тем самым под сомнение наше право на конфиденциальность и безопасное использование цифровых инструментов. Санкционированный правительством надзор с целью обеспечения национальной безопасности может быстро привести к сбору больших объемов данных и хранению персональной информации, что затрудняет проведение различия между приемлемой и неприемлемой практикой, которая воспринимается как заходящая за красную линию.

---

119 Европейский суд по правам человека, дело "Хэндисайв против Соединенного Королевства" http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"dmdocnumber":["695376"],"itemid":["001-57499"]}, последний раз обновлено 17.10.2014 г.

В то же время, чтобы пользоваться наиболее удобным режимом защиты данных, в поисках финансовых и конкурентных преимуществ частный сектор собирает и передает огромные объемы персональных данных через границы, тем самым подвергая их новым рискам.

Учитывая не знающую границ природу интернета, для обеспечения свободы в интернете национальных законов недостаточно. Поэтому столь важно разработать и принять международные рамки для создания кибердоверия.

Настоящая глава состоит из пяти разделов. Во-первых, в ней подчеркивается отсутствие надлежащей правовой основы, что сказывается на защите гражданских свобод в киберпространстве и на свободе в интернете, чему иллюстрацией служит ситуация, сложившаяся в настоящее время во многих странах арабского мира. В следующем разделе рассматривается дискуссия по поводу больших данных и вопрос защиты данных, чтобы показать необходимость международной нормативно-правовой базы для сохранения свободы в интернете и права на конфиденциальность. В третьем разделе речь идет о проблеме надзора и сбора информации государством в киберпространстве и о воздействии этих видов деятельности на стремление создать доверие к использованию киберпространства.

В четвертом разделе обсуждается европейская позиция относительно посягательства правительств на цифровую конфиденциальность и защиту данных, а также значение согласованной в этом отношении политики в Европейском союзе, не только для содействия сотрудничества между его государствами-членами, но и для того чтобы служить примером за его пределами. В заключение в последнем разделе предпринимается попытка установить критерии для управления киберсвободой как одним из основополагающих прав человека и существенным фактором создания кибердоверия.

3.1 Киберсвобода: прогресс и вызовы

Мона Аль-Ашкар

Введение

Мощь новых технологий возвестила эру, где все чаще отбрасываются технические ограничения того, что можно делать на многочисленных уровнях, цифровую эпоху, в которую права и возможности отдельных лиц и государств расширяются, как никогда ранее, не только в отношении развития, но и в отношении распространения в больших масштабах оскорблений и насилия.

Этот парадокс отражается в сопоставлении неоспоримых преимуществ цифровой эпохи с многочисленными опасностями, грозящими отдельным людям, деловому миру и государствам ввиду того, что они все в большей мере полагаются на ИКТ, а

преступная деятельность в киберпространстве становится все более изощренной. Угрозы национальной безопасности становятся серьезнее, и важнейшая инфраструктура все в большей мере подвергается многочисленным рискам, в том числе атакам в интернете.

Наряду с киберпреступностью несовместимость и отсутствие или недостаточная проработанность правовой базы все еще являются основными факторами, подрывающими доверие к использованию платформ киберпространства. Это происходит потому, что они позволяют возникнуть правовой незащищенности и препятствуют полномасштабному осуществлению гражданских свобод. Соответственно, поддержание порядка в интернете создает реальную угрозу многим гражданским свободам, таким как конфиденциальность, свобода выражения мнений, защита от самооговора, несанкционированных обысков и изъятий, а также право на соблюдение процессуальных норм. Уровень защиты этих гражданских свобод во многом зависит от законодательства, правовой практики и политической системы, имеющихся в той или иной стране или регионе.

Защита этих гражданских свобод и создание тем самым доверия в киберпространстве является необходимой предпосылкой обеспечения надежной экономической киберсреды. Это ясно показало дело PRISM, в ходе которого были раскрыты тайный сбор персональных данных и шпионские операции Агентства национальной безопасности США. После обнародования этого корпорация Cisco заявила о снижении доходов на 8–10% и прогнозировала дальнейшее сокращение масштабов деятельности и уменьшение доходов на 2013–2014 годы, как из-за ухудшения экономической ситуации в мире, так и из-за последствий скандала с PRISM.

Такое массовое слежение в сочетании с возникающими понятиями "киберрепрессий" и "электронного полицейского государства" указывают на упадок многих из вышеперечисленных гражданских свобод, как у диктаторских режимов, так и в демократических странах.

Гражданские свободы

Термин "гражданские свободы" происходит от латинского "ius civis", что означает "права граждан"), и восходит к Великой хартии вольностей, предназначением которой было ограничение злоупотребления властью. Поэтому гражданские свободы признаются защитой от незаконной практики и действий правительств и от нарушения ими основных юридических прав.

Тогда как права человека носят универсальный характер и применяются в равной мере ко всем странам, гражданские права связаны с национальным законодательством каждой страны. В соответствии с этим каждая страна предоставляет своим гражданам основные свободы, предусмотренные ее национальной правовой системой. Главное значение гражданских свобод заключается в том, что они ограничивают уровень вмешательства государства в жизнь граждан, а также все виды злоупотребления

властью и тем самым обеспечивают гражданам возможность участвовать в гражданской и политической жизни страны, не подвергаясь дискриминации или репрессиям.

К гражданским свободам относятся такие личные, политические и экономические права, как право на справедливое судебное разбирательство, право на соблюдение законности, свобода собраний, право на ходатайство, право на самооборону, право голоса, свобода от рабства и принудительного труда, свобода от пыток и убийства, право на свободу и безопасность, свобода совести, свобода вероисповедания, свобода выражения мнений, свобода слова, право на неприкосновенность частной жизни, право владеть собственностью, право на вступление в брак, право на самозащиту, право на неприкосновенность личности, право на использование средств, право на равное образование и право участвовать в государственном управлении.

Гражданские свободы, утвержденные национальным законодательством, могут иметь общую правовую базу, такую как гражданско-правовой деликт, дающую частным лицам возможность требовать возмещения – не только от других лиц, но и от правительства, при несправедливом обращении или причинении ущерба из-за нарушения их основных прав. К таким нарушениям относятся, например, несанкционированное вторжение в жилище или нарушение неприкосновенности частной жизни, клевета или незаконное присвоение.

Свобода информации: право на доступ к информации

Свобода информации или право на доступ к информации возникли как новое право, отличное, но неотделимое от права на свободу выражения мнений. Его можно определить как право на доступ к информации, находящейся в распоряжении государственных органов[120].

Согласно итоговому документу собрания экспертов, проведенного Секретариатом Содружества, в котором принимается во внимание Статья 19: "Свобода информации должна гарантироваться как законное и осуществимое право, дающее возможность любому лицу получать сведения и информацию, находящиеся в распоряжении исполнительной, законодательной и судебной ветвей власти, а также любой находящейся в государственной собственности корпорации и любого другого органа, выполняющего государственные функции".

Основной принцип, на котором зиждется эта свобода, заключается в праве граждан знать, обязанности правительства информировать граждан и в том факте, что бремя доказательства возлагается на сторону, которой адресован запрос на информацию. Поэтому в большинстве своем правительства, как правило, делают информацию,

120 http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-information/

которую они не хотят раскрывать, секретной или недоступной по государственным соображениям.

Право на доступ к информации включает право искать, получать и передавать информацию и идеи и охватывает как тех, кто активно занимается поиском информации, так и тех, кто рассчитывает получать ее через СМИ или по официальным каналам. Это право в основном относится к доступу к публичной информации. Это подчеркивает принцип публичности законов, а также прозрачность государственной администрации, что напрямую связывает применение этого права с активным участием граждан в политической жизни и работе механизмов, борющихся с коррупцией.

Согласно резолюции 59 (1) Генеральной Ассамблеи ООН: "Свобода информации представляет собой основное право человека […], критерий всех видов свободы, защите которых Объединенные Нации себя посвятили"[121]. Аналогичным образом в преамбуле Лимских принципов Чапультепекской декларации утверждается, что "[…] право частного лица на свободу выражения мнений и доступ к информации имеют основополагающее значение для существования всех демократических обществ и необходимы для прогресса, благосостояния и осуществления всех других прав человека"[122].

Наряду с этим в Тунисском обязательстве Всемирная встреча на высшем уровне по вопросам информационного общества вновь подтвердила необходимость соблюдения государствами прав человека и основополагающих свобод и признала значение "[…] свободы выражения мнений и свободного потока информации, идей и знаний в информационном обществе"[123].

Таким образом, право на доступ к информации считается основополагающим для осуществления, в том числе, свободы выражения мнений и свободы убеждений. Оно подразумевает обязанность правительств гарантировать свободный поток информации и идей. Абид Хуссейн, бывший в то время Специальным докладчиком ООН по вопросу о праве на свободу мнений и их свободное выражение заявил в своем докладе 1995 года Комиссии ООН по правам человека: "Свобода потеряет всякий смысл, если лишить людей доступа к информации. Доступ к информации является одной из основ демократического общества. Поэтому следует решительно пресекать попытки сокрытия информации от широкой общественности".

---

121 Генеральная Ассамблея ООН (1946 г.), резолюция 59 (1), 65-е пленарное заседание http://foishehri.wordpress.com/.

122 http://www.rjionline.org/MAS-Codes-Peru-Lima-Principles

123 http://www.itu.int/wsis/docs2/tunis/off/7.pdf

Уровни свободы доступа к информации различаются в разных странах. В этом отношении особого внимания заслуживают некоторые происшедшие в последнее события. Так, в некоторых арабских странах после "арабской весны" в конституции[124] было включено положение, гарантирующее право на информацию[125]. Еще один показатель связан с тем, что Закон США о борьбе с терроризмом затрудняет американским гражданам доступ к информации, которой располагает правительство.

Хотя государствам предлагается признавать и соблюдать это право, следует отметить, что оно зачастую ограничивается органами власти, когда считается, что оно препятствует или ставит под угрозу защиту национальной безопасности, территориальную целостность, общественную безопасность, предотвращение преступности, защиту здоровья или морали, а также неприкосновенность частной жизни других лиц, их репутацию или права. Вместе с тем эти ограничения должны определяться в соответствии с законом и требованиями сохранения правовой беспристрастности и надлежащего функционирования демократии.

В киберпространстве свобода информации позволяет частным лицам и организациям пользоваться свободой слова и социальным общением более высокого уровня. В то же время возникает комплекс новых проблем, который может ограничить использование социальных сетей. Наиболее свежими примерами этого являются "арабская весна" и похищенные документы "викиликс". Наряду с проблемами, которые такие случаи создают в отношении национальных интересов и сохранности секретных данных, они также делают более заметными ограничения и практику надзора в интернете со стороны как государств, так и объединений частного сектора.

На основании принятого в 2004 году Группой восьми обязательства содействовать развитию среды, благоприятной для неофициального, открытого и охватывающего всех диалога, в том же году страны Ближнего Востока и Северной Африки начали осуществление инициативы "Форум будущего". Вслед за этим в июле 2008 года организации гражданского общества из Бахрейна, Египта, Иордании и Марокко создали Арабскую сеть свободы информации. Но, несмотря на ведущуюся в регионе информационно-пропагандистскую деятельность, прогресса в большинстве арабских стран в области законодательства по свободе информации достичь не удалось. Иордания и Тунис остаются единственными арабскими государствами, принявшими закон о доступе к информации, хотя подобные законопроекты обсуждались в Бахрейне, Египте, Кувейте, Ливане, Марокко, Палестине и Йемене. В Ливане в 2004 году при помощи Американской ассоциации юристов был подготовлен группой ливанских юристов законопроект о защите лиц, сообщающих о злоупотреблениях,

---

124 http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f

125 http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f

который был представлен в ливанский парламент в 2010 году Национальной сетью за право доступа к информации в Ливане.

Неприкосновенность частной жизни: защита от всемирного разведывательного сообщества

Неприкосновенность частной жизни – это гражданская свобода, непосредственно связанная с личными свободами, достоинством и телесной неприкосновенностью. Ее суть – право граждан на защиту от несанкционированного вмешательства государства в их жизнь, такого как несанкционированные обыски жилищ и слежение за перепиской/общением. В цифровой век неприкосновенность частной жизни рассматривается в новом контексте. Она больше не сводится к защите физического и материального окружения, такого как жилище, почта или документы, и охватывает огромный объем персональных данных в киберпространстве, как и высокий уровень возможности установления соединений, который превращает каждого в "датчик всемирного разведывательного сообщества"[126].

На глобальном уровне не существует договоренности относительно того, что может считаться адекватной защитой неприкосновенности частной жизни. Вместе с тем имеется базовая международная правовая основа для права на неприкосновенность частной жизни, которую можно распространить на киберпространство и в которой отражены положения международного, региональных и национальных законодательств, деклараций, конвенций и договоров.

В Статье 12 Всеобщей декларации прав человека неприкосновенность частной жизни признается одним из основополагающих прав человека. Согласно этой Декларации, никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию, и каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств.

Статья 17 Международного пакта о гражданских и политических правах гласит: "Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию, и, следовательно, каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств".

---

126 Филипп Ланглуа, основатель базирующейся в Париже компании Priority One Security, о способности учреждений собирать персональные данные пользователей смартфонов.
http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0

К числу других соответствующих руководящих указаний, конвенций и директив относятся:

- "Директивы в отношении охраны тайны и трансграничных потоков персональных данных" 1980 года, выпущенные Организацией экономического сотрудничества и развития;
- "Конвенция о защите физических лиц при автоматизированной обработке персональных данных" 1981 года, выпущенная Советом Европы;
- "Руководящие указания по использованию автоматизированного потока персональных данных" 1989 года, выпущенные Советом Европы;
- "Руководящие принципы регламентации компьютеризированных картотек, содержащих данные личного характера" 1999 года, ООН.

В этих документах устанавливаются принципы минимальных гарантий конфиденциальности информации личного характера на всех стадиях ее обработки (сбор, хранение, распространение, использование, передача и т. д.). В них также признается право частного лица на доступ к своим персональным данным, их обновление и информирование о методах и целях операций по сбору данных. Наряду с этим в них устанавливается право частного лица уничтожать свои данные после установления цели их сбора и обработки, что служит поддержкой права быть забытым в сети. На региональном уровне некоторые страны уже приняли меры и ввели минимальные уровни надлежащей защиты в отношении вопросов конфиденциальности.

Директива ЕС 1995 года о защите данных допускает сбор данных личного характера для конкретных, ясно выраженных и законных целей и запрещает сохранение данных, которые не являются актуальными, важными и точными. Наряду с этим государства – члены ЕС обязаны не допускать передачи этих данных за рубеж[127] при отсутствии эквивалентных мер, обеспечивающих защиту данных и права граждан на доступ, защиту, изменение их данных и отказ в праве на их использование какой-либо третьей стороной.

Так, чтобы разрешить трансграничный поток данных в США, где такой уровень надлежащей защиты отсутствует, ЕС заключил с этой страной Соглашение о безопасной гавани. Это соглашение дает некоторым компаниям США право собирать данные о гражданах ЕС, при условии что они могут доказать, что ими принимаются меры для обеспечения защиты этих данных в соответствии со стандартами ЕС. К тому

---

127 Директива 95/46/ЕС Европейского парламента и Совета от 24 октября 1995 года о защите частных лиц в отношении обработки данных личного характера и свободного перемещения таких данных – *Official Journal L 281, 23/11/1995 P. 0031 – 0050*.

(57) Тогда как, с другой стороны, передача данных личного характера третьей стране, которая не обеспечивает надлежащего уровня защиты, должна быть запрещена;

же эти компании должны уведомлять соответствующих граждан ЕС о том, как обрабатываются и используются их данные, а также признавать их права на получение доступа к данным, их отзыв и изменение.

На региональном уровне Директива ЕС о защите данных регулирует свободное перемещение персональных данных между членами ЕС и обязывает включить свои положения в национальное законодательство, разрешая при этом отдельным странам ЕС применять собственные подходы к ее реализации. Субъектам данных должно гарантироваться право знать, откуда происходят данные, право исправлять неточные данные, право подавать жалобы в случае незаконной обработки и право отказывать в разрешении на использование данных в определенных обстоятельствах.

На национальном уровне почти все страны признают конституционное право на неприкосновенность частной жизни. В некоторых вновь принятых конституциях (Южная Африка) и во многих европейских странах утверждены законы, регулирующие надзор за персональными данными защищающими неприкосновенность частной жизни граждан[128]. ООН поддержала защиту неприкосновенности частной жизни, одобрив проект резолюции[129], подготовленный Бразилией и Германией и озаглавленный "Право на неприкосновенность личной жизни в цифровой век"[130].

Свобода выражения мнений: отличительная черта демократического общества

В демократическом обществе законодательство, свобода слова и независимое гражданское общество служат защите свободы вообще и демократических свобод, тогда как отличительными чертами деспотичных режимов являются безнаказанность действий полиции, несправедливые судебные разбирательства и произвольное задержание.

Согласно Статье 19 Всеобщей декларации прав человека, а также Статье 19 Международного пакта о гражданских и политических правах: " Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает

---

128 Закон 2008 года о поправках к Закону о наблюдении за иностранной разведкой, Закон о прослушивании (Communications Assistance for Law Enforcement Act), США.

Закон о защите данных 1998 года и Закон о полномочиях властей, расследующих уголовные преступления (RIPA) в Соединенном Королевстве – Закон 1978 года об информатике и гражданских свободах во Франции – Конвенция ЕС о защите персональных данных, Директива ЕС о сохранении данных.

129 Генеральная Ассамблея поддерживает право на неприкосновенность частной жизни в цифровой век.

http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY

130 Шестьдесят восьмая сессия – Третий комитет – Пункт 69 (b) повестки дня – Поощрение и защита прав человека: вопросы прав человека, включая альтернативные подходы в деле содействия эффективному осуществлению прав человека и основных свобод.

свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ". Свобода выражения убеждений означает способность свободно выражать идеи и мнения по экономическим, политическим, социальных и другим вопросам всеми имеющимися средствами общения – например, письменно, в живописи, вещании или блогах. В соответствии с этим свобода печати и свобода использования социальных сетей являются частью данной свободы.

Аналогичным образом, Статья 11 Хартии ЕС по правам человека, соответствующая Статье 10 Европейской конвенции о правах человека, гласит: "Каждый имеет право свободно выражать свое мнение. Это право включает свободу придерживаться своего мнения и свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ. Далее в ней говорится: "Осуществление этих свобод, налагающее обязанности и ответственность, может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного порядка, в целях предотвращения беспорядков и преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия". Вместе с тем, как при всех ограничениях прав и свобод, в ней признаются принципы необходимости и пропорциональности, а также необходимости воздерживаться от произвольных или дискриминационных видов практики.

В соответствии с этим свобода выражения мнений считается одним из основных элементов обеспечения доверия граждан к правительству и политической системе, осуществления других прав человека, лучшего понимания государственной политики, создания должным образом информированного общественного мнения и свободы выражения мнений по волнующим вопросам в СМИ. На национальном уровне свобода выражения мнений во многих конституциях признается отличительной чертой демократических режимов. В этом контексте Генеральная Ассамблея ООН считает, что контролирование сетей электросвязи ставит под угрозу права человека и многие гражданские свободы, от свободы убеждений и их выражения до права на

неприкосновенность частной жизни и политическую активность, и что оно подрывает основы демократического общества[131].

Таким образом, необходимо соблюдать свободу выражения мнений в онлайновой среде, и ожидается, что правительства будут воздерживаться от ее подавления и будут устранять любые препятствия в этом отношении. В частности, что касается цели настоящей публикации, ожидается, что они будут воздерживаться от киберрепрессий, подавляющих голоса оппозиции, и от перехвата сообщений, цензуры контента и блокирования веб-сайтов.

В то же время на практике свобода выражения мнений не соблюдается во многих странах. Некоторые правительства ссылаются на защиту религиозных ценностей и приличий, в дополнение к национальной безопасности и борьбе против терроризма, как на основания для ограничения свободы выражения мнений в онлайновой среде. Они подвергают цензуре контент, который считают сексуально откровенным, или который пропагандирует ненависть на основании расы, религии либо иных культурных факторов, или который способствует террористической деятельности. Опасность кроется в юридической терминологии, используемой для порицания такого контента, которая обычно применяется расширительно, то есть может не обладать объективностью и стабильностью правосудия, тем самым приводя к злоупотреблению властью.

Социальные сети

Обсуждение, обмен мнениями и формулирование общих целей, как и лоббирование обычно являются предварительными шагами при организации протестов, которые иногда приводят к революции. Масштабы обсуждения в социальных сетях свободы интернета и демократии, в сочетании с растущей способностью граждан оказывать влияние на национальную политику сыграли решающую роль в формировании политических дебатов в ходе "арабской весны". Это создало благоприятную новую среду с помощью постов в блогах, твитов и закачек в YouTube. Как сказал один египетский активист: "Интернет заслуживает самой тщательной защиты от правительственного вмешательства. Если хотите освободить людей, дайте им интернет".

---

131 Генеральная Ассамблея ООН – 16 мая 2011 года – A/HRC/17/27 – Совет по правам человека – Семнадцатая сессия – Пункт 3 повестки дня – Поощрение и защита всех прав человека, гражданских, политических, экономических, социальных и культурных прав, включая право на развитие "Рост использования и сложности цифрового надзора превышает способность общества придать законодательную форму его надлежащему применению, что приводит "к появлению произвольной практики слежения, которая находится вне контроля независимых органов" и создает угрозу подавления свободного выражения мнений".

Социальные сети дают возможность мобилизации людей, а также тайного обмена информацией, ранее не существовавшего. Они открывают широкие перспективы организации и передачи информации и могут помочь сформировать оппозиционные группы и выстроить их структуру, привлечь активистов, обратиться к сочувствующим, распространять идеологию и создавать как внутренние, так и внешние сети поддержки. Во время "арабской весны" активисты использовали социальные сети для получения поддержки на региональном и международном уровнях, а также для организации пропагандистских кампаний.

Хотя социальные сети не могут заменить физические действия, необходимые для подготовки успешных революций, они дали гражданам арабских государств возможность использовать информацию как мощное оружие против репрессий. Участники движений "арабской весны" использовали социальные сети для поддержания контактов, обмена информацией, распространения сообщений о реальных событиях, организации своей деятельности, распространения информации и новостей, обращения к миру и оказания влияния на общественное мнение. Изображения и видеоматериалы, отправляемые с мобильных телефонов, помогали в сборе информации о правительственных силах и их позициях. В основном политические действия организовывались и пропагандировались в социальных сетях. До смены режимов в ходе "арабской весны" в нескольких арабских странах твиты групп оппозиции стремительно распространялись и достигали миллионов зрителей и страниц Facebook. Резко выросли число блогов, порождая в регионе обсуждение вопросов демократии, свободы и прозрачности. Миллионы граждан пользовались социальными сетями, и было создано множество страниц и сайтов для содействия информационно-пропагандистской работе оппозиции посредством онлайновых сообщений и блогов. Используя свои сотовые телефоны, некоторые активисты обеспечивали освещение событий в режиме реального времени и размещали материалы в Facebook, Twitter и других социальных сетях. Сегодня многие из лозунгов того времени часто используются в других странах в ходе различных социальных, политических и экономических протестов.

Вызывающие беспокойство нападки на свободу выражения мнений участились в Ливане за последний год. Его репутации как оплота свободы слова повредила череда арестов, задержаний и устрашения ливанских граждан в связи с их онлайновой деятельностью, в первую очередь в социальных сетях.

Политики в Ливане, похоже, все чаще занимают оборонительные позиции, поскольку их, по-видимому, задевают состоящие из 140 символов твиты и иной контент социальных сетей. Так, были арестованы четыре пользователя Facebook, а один пользователь Twitter был приговорен к двум месяцам тюремного заключения за оскорбление президента республики. Еще в одном деле блоггеру, задержанному более чем на восемь часов, грозили судебным преследованием, если он не перестанет писать о политике и не ограничится сочинением стихов. Нескольких блоггеров допрашивали органы борьбы с киберпреступностью, а некоторые блоги были

блокированы, в том числе пост о несправедливом обращении с работниками крупной сети супермаркетов.

Такие решения, схожие с санкциями в странах с деспотическими режимами, в прошлом были редкостью в Ливане, где регулирование выражения мнений ранее применялось в сравнительно небольших масштабах.

Опасности: факты и субъекты

Киберпространство представляет собой новое измерение национальной безопасности и является ценным источником информации для сбора разведывательных данных. Но традиционные способы контролирования и сбора информации органами безопасности более не являются адекватными.

В настоящее время требуется выявлять и обнаруживать заговорщиков и предвидеть действия в сетях, которые могут носить злонамеренный и преступный характер. С этой целью применяются сложные технологии для массового наблюдения за компьютерными сетями и их пользователями для обнаружения, выявления и отслеживания тех, кто в них вторгается, и для сохранения данных на основе свидетельств.

Вопросы сбора персональных данных и связанные с этим нарушения гражданских свобод широко освещаются в средствах массовой информации во всем мире; разоблачения Сноудена, WikiLeaks и Tempora[132], в частности, привели к ужесточению контроля над сетью посредством СОРМ-2 и СОРМ-3[133], единого реестра[134] и цензуры в

---

132 Tempora представляет собой секретную программу электронного наблюдения в целях обеспечения безопасности, которая была испытана в 2008 году[2], внедрена в 2011 году и используется Центром правительственной связи Великобритании (GCHQ). Tempora использует перехват сообщений, передаваемых по волоконно-оптическим кабелям, образующим магистральную сеть интернета, для получения доступа к большим объемам персональных данных пользователей интернета, http://en.wikipedia.org/wiki/Tempora.

133 Эти законы, как представляется, противоречат статье 23 Конституции России, которая гласит[32]:

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

134 In Ex-Soviet States, Russian Spy Tech Still Watches You- By Andrei Soldatov and Irina Borogan – 12.21.12 6:30 AM, http://www.wired.com/dangerroom/2012/12/russias-hand/all/.

социальных сетях[135]. В последнее время некоторые правительства усилили контроль над интернетом с помощью мер по обеспечению онлайновой идентификации пользователя[136].

Органы безопасности могут получать доступ к персональным данным и сверять их со списками объектов разведки. Технологии наблюдения позволяют им определять местонахождение объектов с использованием карт Google, или GPS-систем слежения за перемещениями, или компонентов, которые встраиваются в изображения, размещаемые в социальных сетях. Используя такие технологии, они могут также получить списки адресов и распечатки с телефонов членов семьи и друзей посредством записи и хранения сообщений электронной почты. Согласно секретным документам британской разведки, шпионы скрываются даже за популярными игровыми приложениями, стремясь получить данные о местонахождении, возрасте, половой принадлежности и другую персональную информацию игроков.

Это явление в значительной мере ослабляет неприкосновенность частной жизни и многих гражданских свобод. Однако угрозы неприкосновенности нашей частной жизни и другим гражданским свободам исходят не только от правительств. Незаконное наблюдение за людьми ведется как государственными, так и частными субъектами, поскольку оно может быть полезным как для целей маркетинга, так и для сбора разведывательных данных. Большие и малые корпорации следят за тем, что мы покупаем, собирают персональные данные для рассылки людям адресной рекламы на мобильные телефоны, хранят и анализируют данные и используют их в коммерческих целях. Иногда они осуществляют сбор особо конфиденциальных данных, которые они называют необязательными и которые, в частности, касаются этнической принадлежности и сексуальной ориентации.

Государственная цензура осуществляется с помощью таких мер, как фильтрация интернета, использование вредоносных мониторинговых программ типа троянских программ[137] и ограничения анонимности в интернете. Эти меры направлены на содействие надзору государства за связью путем упрощения идентификации лиц, получающих доступ к запрещенному контенту или распространяющих его, и на сбор разведывательных данных.

---

135 King, Gary, Jennifer Pan, and Margaret Roberts. 2014. Reverse Engineering Chinese Censorship through Randomized Experimentation and Participant Observation. Копия содержится по адресу http://j.mp/16Nvzgehttp://gking.harvard.edu/publications/randomized-experimental-study-censorship-china.

136 Китай требует регистрации под подлинными именами при выкладывании видеоматериалов в сеть, http://www.reuters.com/article/2014/01/21/us-china-internet-idUSBREA0K04T20140121.

137 Приложение QQ в Китае, которое считается гигантской троянской программой.

Масштабы сбора данных и перехвата сообщений являются весьма впечатляющими и обескураживающими и представляют серьезную опасность для неприкосновенности частной жизни и гражданских свобод.

Тем не менее очевидны и некоторые позитивные аспекты этого наблюдения. Например, наблюдение позволило сорвать планы "Аль-Каиды" по организации взрывов в Германии в 2007 году и арестовать лиц, стоявших за сетями распространения наркотиков[138] и детской порнографии[139]. В этом контексте можно также упомянуть европейский проект INDECT "Интеллектуальная информационная система, поддерживающая наблюдение, поиск и обнаружение в целях обеспечения безопасности граждан в городской среде", который призван обеспечить безопасность граждан, главным образом в отношении насилия.

В центре внимания – страны арабского мира[140]

Большинство арабских стран являются членами ООН, и все они состоят в Лиге арабских государств, в которую входят независимые арабские государства Северной и Северо-Восточной Африки и Юго-Западной Азии. Цель Лиги заключается в укреплении отношений между государствами-членами, содействии сотрудничеству между ними и защите их независимости и суверенитета. Конкретнее, она имеет целью укрепление тесного сотрудничества в экономической и финансовой сферах, сферах связи и здравоохранения, социальной и культурной сферах, а также в вопросах, относящихся к гражданству, паспортам, визам, исполнению судебных решений и выдаче преступников.

Арабские страны обязуются уважать свободу выражения мнений в соответствии со статьей 19 Всеобщей декларации прав человека и статьей 32 Арабской хартии прав человека, основанной на вышеупомянутой статье 19.

Объявленными причинами для введения ограничений и наказаний, как правило, являются общественные нравы и традиции, а также религия. Некоторыми странами приняты чрезвычайные законы, которые всегда направлены на подавление инакомыслия посредством преследования тех, кто отваживается свободно высказывать свое мнение. Они могут быть подвергнуты грубому аресту, пыткам и

---

138 Drug lord Guzman arrested, http://news.yahoo.com/internet-crucial-venezuela-battleground-075124059.html.

139 How the NSA's High-Tech Surveillance Helped Europe Catch Terrorists, http://www.civilbeat.com/articles/2013/06/21/19341-how-the-nsas-high-tech-surveillance-helped-europe-catch-terrorists/.

140 Страны арабского мира здесь определяются как страны – члены Лиги арабских государств: Алжир, Бахрейн, Джибути, Египет, Йемен, Иордания, Ирак, Катар, Коморские Острова, Кувейт, Ливан, Ливия, Мавритания, Марокко, Объединенные Арабские Эмираты, Оман, Палестинские территории, Саудовская Аравия, Сирия (членство приостановлено), Сомали, Судан и Тунис.

тюремному заключению за преступление, заключающееся в принадлежности к "незаконной организации", измену или заговор против национальной безопасности и национальных интересов. Некоторые правительства создают или расширяют свои возможности по ограничению гражданских свобод, используя прокси-серверы компании Blue Coat и иностранные технологии для отслеживания и блокирования сообщений диссидентов.

Широко практикуется цензура в интернете, хотя правительства утверждают, что цензуре подвергаются только порнографические сайты. Пользователей могут направлять на прокси-сервер со списком запрещенных веб-сайтов, который блокирует материалы, считающиеся несовместимыми с местными религиозными, культурными, политическими и моральными ценностями. Большинство журналистов и блогеров прибегают к самоцензуре, особенно по таким вопросам, как местная политика, культура, религия или любой другой вопрос, который может быть сочтен властями острым с политической или культурной точки зрения. В целом они стараются не критиковать главу государства или других должностных лиц и не публиковать информацию, которая потенциально могла бы нанести вред репутации страны, ее внешним связям или национальной экономике. Клевета является уголовным преступлением.

В одном получившем широкий общественный резонанс случае в Объединенных Арабских Эмиратах в 2009 году независимый журналист Марк Таунсенд, бывший редактор отдела деловых новостей издающейся в Дубае англоязычной газеты "Халидж таймс", был обвинен в преступной клевете и после этого в течение почти двух лет не мог покинуть страну, пока велось расследование. Ему было предъявлено обвинение по статье 373 уголовного кодекса за предполагаемую публикацию статей с критикой в адрес газеты "Халидж таймс", 30% акций которой принадлежат государству, и грозило наказание в виде тюремного заключения на максимальный срок до двух лет и штраф в размере 20 000 дирхамов (5400 долларов США). В конечном счете, в мае 2011 года он был оправдан. В другом случае, имевшем место в 2011 году, пять активистов и блогеров из Объединенных Арабских Эмиратов были арестованы и обвинены в оскорблении лидеров страны в размещенных на интернет-форуме UAE Hewar постах. Они были приговорены к тюремному заключению.

Из более позитивного стоит отметить, что интернет стал пространством для организации и лоббирования среди активистов. Однако при этом правительства арабских стран отключают интернет в случае вспышки антиправительственных гражданских демонстраций.

Неприкосновенность частной жизни в арабском мире воспринимается главным образом в физическом и материальном плане. Основной акцент делается на таких факторах, как неприкосновенность жилища, тайна личной корреспонденции и неприкосновенность средств связи. Однако в правовых системах арабских стран отсутствует надлежащая защита права на неприкосновенность частной жизни, за

исключением редких случаев, когда такая защита обеспечивается конституцией или сводами законов.

В Ливане неприкосновенность частной жизни не имеет четко определенного правового статуса, хотя эта тема широко обсуждается политическими лидерами. Ее защита обеспечивается совокупностью конституционных и законодательных положений. В конституции Ливана, подобно конституции США, нет определения права на неприкосновенность частной жизни. Тем не менее она гарантирует защиту личности и защиту жилища и личного имущества.

Некоторые положения обеспечивают защиту людей от распространения информации об их личной жизни в определенных особых обстоятельствах. В статье 17 говорится, что жилище неприкосновенно и что никто не вправе проникать в него иначе как в особых обстоятельствах и с соблюдением регламента, установленного законом. Кроме того, согласно закону о перехвате информации граждане имеют право на неприкосновенность своих средств местной или международной проводной или беспроводной связи.

В конституции Ливана признается право на защиту личности, жилища, бумаг и имущества от необоснованных обысков и арестов, которые возможны только в случае их санкционирования в предписанных законом условиях. По примеру правительств многих стран мира в Ливане в качестве законного основания для вмешательства в частную жизнь и нарушения при этом многих гражданских свобод всегда используются такие причины, как национальная безопасность, борьба с терроризмом и защита общественного благополучия.

Аналогичные причины приводятся для оправдания блокирования правительством социальных сетей в интернете, которые иногда используются для пропаганды и организации протестных мероприятий в странах арабского мира.

В марте 2013 года организация "Репортеры без границ" назвала несколько арабских стран "государствами – врагами интернета"[141] из-за применяемых ими методов, таких как жесткие преследования блогеров, приводящих к серьезным нарушениям свободы информации и прав человека.

Лига арабских государств и гражданские свободы

Лига арабских государств была учреждена за семь месяцев до создания Организации Объединенных Наций шестью странами (Египтом, Ираком, Ливаном, Саудовской Аравией, Сирией и Трансиорданией), и в настоящее время насчитывает двадцать два арабских государства-члена.

---

141 Reporters Without Borders' March 2013 – Special report on Internet surveillance, titled "Enemies of the Internet" focusing on 5 governments and 5 companies, http://en.rsf.org/special-report-on-internet-11-03-2013,44197.html.

В уставе, принятом при учреждении Лиги в 1945 году, не было ссылок на права человека. Кроме того, в правовых документах Лиги арабских государств нет конкретных положений о защите правозащитников.

С другой стороны, Лига создала комитет в целях разработки более комплексной и согласованной правовой системы на основе унификации юридических и судебных терминов, структур и процессов. Для выполнения рекомендаций этого комитета Лигой был учрежден Арабский центр юридических и судебных исследований в Бейруте. Центр разработал большое число конвенций, касающихся сотрудничества арабских стран по многим представляющим общий интерес правовым вопросам, как, например, типовое законодательство по борьбе с киберпреступностью. Он сотрудничает со многими международными и региональными организациями, а также с организациями гражданского общества по вопросам управления использованием интернета. Так, совместно с ЭСКЗА ООН он занимался вопросами создания и официального открытия Арабского форума по управлению использованием интернета. Кроме того, с 2009 года он является одним из членов – основателей Панарабского центра наблюдения за кибербезопасностью и инициировал разработку проекта арабской конвенции по кибербезопасности, которая должна быть представлена Совету министров юстиции арабских стран. В проекте прямо говорится о защите гражданских свобод в интернете как об одном из важнейших элементов укрепления доверия при использовании киберпространства. В то же время Центр открыл много форумов и ежегодных собраний для лиц, принимающих решения в области ИКТ по вопросам, связанным с правами человека и гражданскими свободами, в частности правами на неприкосновенность частной жизни, доступ к информации и свободу выражения мнений.

Заключение

Для того чтобы обеспечить надлежащий баланс между необходимостью защиты гражданских свобод, неприкосновенности частной жизни пользователей интернета и, в первую очередь, свободы выражения мнений и необходимостью противодействия киберугрозам национальной безопасности нужны согласованные усилия законодательных органов. Успех в этом отношении помешал бы превращению киберпространства в новую сферу надзора.

Государства должны осуществлять преследование за киберпреступления как за уголовные преступления согласно национальному закону, в котором должно быть обеспечено сочетание предупредительных ответных мер для защиты гражданских свобод. Защите неприкосновенности частной жизни при обмене информацией способствовали бы специальный международный договор или соглашение, предусматривающие разумный минимальный уровень защиты, приемлемый для всех заинтересованных сторон. Они должны быть дополнены эффективным механизмом международного сотрудничества в целях борьбы с транснациональной киберпреступностью. В этой связи Центр юридических и судебных исследований Лиги

арабских государств обратился ко мне с просьбой подготовить проект арабской конвенции о сотрудничестве в целях борьбы с трансграничной киберпреступностью.

В рамках этого механизма сотрудничества расследования, слежение, уголовное преследование, взаимная правовая помощь и судебные разбирательства должны осуществляться в соответствии с национальными законами. Аналогичным образом любые официально утвержденные процедуры обеспечения применения международного права должны использоваться в соответствии с внутренним законодательством и договорами о взаимной правовой помощи. Государства должны ввести в действие специальные процедуры и меры для защиты международного обмена конфиденциальной информацией и для контролирования компьютерных сетей, а также для сбора и обработки данных. Это особенно необходимо в странах, в которых отсутствует надлежащий уровень законодательства о неприкосновенности частной жизни.

Особое внимание следует уделять защите от незаконных обысков и арестов. Технический характер киберпространства вкупе с растущим уровнем киберпреступности и отсутствием соответствующего механизма международного уголовного права осложняют задачу обеспечения соблюдения гражданских свобод.

В большинстве национальных правовых систем действия полиции регулируются конституцией, законодательством и процедурами, обеспечивающими защиту граждан от злоупотребления властью и неправомерных действий со стороны правоохранительных органов, например несанкционированных обысков и арестов и нарушения гражданских свобод при проведении таких операций.

Поскольку во многих странах все еще отсутствуют законы и процедуры, касающиеся киберпространства, а в отношении вопросов кибербезопасности применяются общеуголовные законы, правительства этих стран могли бы в качестве альтернативы принять руководящие принципы, направленные на предотвращение нарушения гражданских свобод в этой сфере. В таких руководящих принципах, в частности, должно быть четко определено, что служит основанием для проведения законных обысков и арестов в рамках обоснованных исключений из требований соблюдения гражданских свобод. Разработчики таких принципов могли бы руководствоваться принятыми в обычном праве исключениями, связанными с "доктриной открытого вида" или "обстоятельствами, не терпящими отлагательства".

Такие исключения могли бы компенсироваться различными защитными мерами – использованием шифрования, анонимных ремейлеров, защищенной анонимной связи, брандмауэров и прокси-серверов. Многие из этих технологий обеспечивают защиту от киберпреступлений, а также повышают конфиденциальность.

3.2 Правовые, политические и регуляторные рамки свободы в интернете и больших данных

Паван Дуггал

Введение

В сегодняшнем динамичном мире в результате экспоненциального роста киберпространства произошли радикальные изменения. Благодаря интернету география стала предметом истории, однако эта порожденная киберпространством среда без границ вызывает огромную обеспокоенность правительств всех стран мира. Именно по этой причине вопрос создания надлежащих политических и регуляторных рамок для киберпространства приобрел столь острый неотложный характер.

Интернет полностью покоится на фундаменте из данных и информации в электронном виде. В сущности термины "данные" и "информация" используются взаимозаменяемо и обозначают строительные блоки, которые необходимы для создания архитектуры контента и которые также лежат в основе каналов связи в интернете.

В своем развитии интернет прошел большой путь от Сети связи управления перспективных научно-исследовательских проектов (ARPANET) в конце 1960-х годов до Всемирной паутины и далее до социальных сетей и социальных, мобильных, аналитических и облачных технологий (технологий SMAC) нашего времени. Интернет стал великим уравнителем, поскольку он предоставляет свободу доступа к информации всем пользователям и бесчисленным множеством способов помогает им решать повседневные проблемы и облегчает различные аспекты их деятельности.

В интернете генерируются огромные объемы данных. Бывший председатель совета директоров компании Google Эрик Шмидт заявил в 2010 году, что за каждые два дня "[…] мы создаем сейчас столько информации, сколько успели создать с момента зарождения цивилизации до 2003 года – порядка пяти эксабайтов данных". Подтверждая этот ошеломительный рост, компания IBM заявляет, что каждый день мы генерируем 2,5 квинтиллиона байтов данных – "[…] столько, что 90% данных в сегодняшнем мире создано лишь за последние два года"[142]. Еще одно свидетельство этого явления отражено в статистических данных, содержащихся в отчете IDC-EMC, в котором указывается, что цифровая вселенная более чем удваивается каждые два года и достигнет 40 000 эксабайтов (40 триллионов гигабайтов) к 2020 году[143]. В своем

142 http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

143 http://www.baselinemag.com/analytics-big-data/slideshows/surprising-statistics-about-big data.html#sthash.COE9uzq6.dpuf, последний раз обновлено 4 августа 2014 года.

прогнозе на 2012 год журнал Economist сообщил, что объем цифровых данных в мире возрос со 130 эксабайтов в 2005 году до 1227 эксабайтов в 2010 году, а в 2015 году прогнозируется его рост до 7910 эксабайтов[144]. Опасения по поводу этих огромных объемов данных усиливаются в связи с появлением в цифровой экосистеме больших данных.

В настоящей статье рассматриваются правовые, политические и регуляторные рамки свободы в интернете и больших данных.

Определение

Прежде чем продолжить рассмотрение правовых и регуляторных вопросов, относящихся к свободе в интернете, следует ознакомиться с различными определениями этого термина, предлагаемыми различными учеными и юристами.

Определение свободы в интернете – большая и вызывающая споры тема; общепринятого определения этого термина не существует. Президент Обама как-то сказал: "Интернет открыл путь инновациям, создал возможности для роста и способствовал свободе быстрее и в больших масштабах, чем любое другое техническое достижение в истории человечества. Его сила в его независимости. Интернет предлагает беспрецедентно свободную от вмешательства правительства систему связи"[145]. Он, в частности, добавил: "Свобода в интернете несовместима с регулированием сетевого нейтралитета и предполагает беспрецедентную свободу от вмешательства правительства".

Дерек Бамбауэр, профессор права в Аризонском университете, говорит: "Вероятно, в конечном счете "свобода в интернете" является термином, от которого следует отказаться, поскольку он носит слишком общий характер и не может быть полезным. Вместо этого странам, культурам и пользователям необходимо попытаться разобраться с трудными компромиссами, которые предполагают связь через интернет"[146].

Вот как определяет свободу в интернете на своем веб-сайте марксистская организация по вопросам средств массовой информации Free Press: "Свобода в интернете означает, что поставщики услуг интернета (ПУИ) не могут осуществлять дискриминацию в

---

144 Welcome to the yotta world', The Outlook for 2012, Economist, Dec. 2011; http://www.economist.com/node/21537922.

145 http://freestatefoundation.blogspot.in/2012/08/the-true-meaning-of-internet-freedom.html

146 Bambauer, D., The Enigma of Internet Freedom, eJournal USA, Vol.15, No.6, 2010, pp. 4-6, см. также http://www.wseas.us/e-library/conferences/2013/Dubrovnik/ECC/ECC-38.pdf, последний раз обновлено 8 августа 2014 года.

отношении различных видов онлайнового контента и приложений"[147].·На веб-сайте Dictionary.com сетевой нейтралитет определяется как принцип, согласно которому основные протоколы Интернет должны быть недискриминационными, в частности операторы интернета должны обеспечивать одинаковый режим для поставщиков контента.

Свобода в интернете означает открытый выбор

В то время как у радиовещательных организаций и компаний подвижной телефонной связи имеются выданные государством лицензии на определенные участки радиочастотного спектра, другие полосы частот являются открытыми, а это значит, что любая компания может разработать такой продукт, как, например, беспроводный домашний телефон, гарнитура Bluetooth, детский монитор или пульт дистанционного управления, использующий это открытое пространство без необходимости в получении какой-либо лицензии от государства[148].

Свобода в интернете приносит не только свободу доступа к этой среде, но и свободу выражения мнений. Однако что более важно, она означает свободу облегчать жизнь людей с учетом различных возможностей, обеспечиваемых интернетом.

Характерные особенности

Некоторые ученые пришли к выводу, что свобода в интернете включает ряд основных свобод, таких как свобода слова, право на неприкосновенность частной жизни, свобода на инновации и на получение вознаграждения и признания, а также свободу архитектуры интернета в целом[149].

Существующие политические и регуляторные рамки

Несмотря на развитие интернета как глобальной среды без границ, фактом остается то, что мир пока не акцентировал внимание на разработке международно признанных норм, конкретно применимых к киберпространству. Поэтому когда речь заходит о правовых, политических и регуляторных рамках, важно отметить, что каких-либо международных договоров о свободе в интернете не существует. Однако в этом направлении есть некоторые подвижки.

---

147 http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/

148 http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/

149 Neelie Kroes, *Internet Freedom,* http://europa.eu/rapid/press-release_SPEECH-12-326_en.pdf, последний раз обновлено 8 августа 2014 года.

Как упоминалось ранее в настоящем отчете, Конвенция Совета Европы о киберпреступности 2001 года служит ярким примером в этом отношении. Характерными особенностями этой Конвенции являются следующие:

- это первый международный договор, направленный на борьбу с киберпреступностью посредством унификации соответствующих национальных законов, обеспечения единых определений некоторых уголовных преступлений, совершенствования методов расследования и расширения сотрудничества "в максимально возможной степени" между странами в целях борьбы с этим явлением[150];
- Конвенция требует введения уголовной ответственности за такие деяния, как хакерство и правонарушения, связанные с детской порнографией, и распространяет уголовную ответственность на нарушения прав интеллектуальной собственности;
- она предусматривает общую политику в области уголовного права, направленную на защиту общества от киберпреступности, на основе принятия соответствующего законодательства и укрепления международного сотрудничества[151].

Декларация о свободе коммуникаций в системе Интернет, принятая Советом Европы в 2003 году, является еще одним ярким примером этих усилий. Ниже отмечаются основные особенности этой Декларации:

- в ней говорится, что государства должны обеспечить баланс между свободой выражения мнений и информации и другими законными правами и интересами в соответствии со статьей 10 Конвенции о защите прав человека и основных свобод;
- в ней высказывается обеспокоенность попытками ограничить доступ общественности к коммуникациям в системе Интернет по политическим или иным мотивам, противоречащим демократическим принципам;
- в ней утверждается, что предварительный контроль за сообщениями в интернете, независимо от границ, должен оставаться исключением;
- в ней принимается во внимание, что существует необходимость в устранении барьеров на пути индивидуального доступа к интернету и вследствие этого в дополнении мер, уже принятых в целях создания пунктов коллективного доступа;

---

150 http://en.wikipedia.org/wiki/Convention_on_Cybercrime, последний раз обновлено 8 августа 2014 года.

151 http://epic.org/privacy/intl/ccc.html

- в ней высказывается убежденность в том, что свобода организации услуг, предоставляемых через интернет, будет способствовать гарантированию права пользователей на доступ к плюралистическому контенту из разнообразных внутренних и внешних источников;
- в ней подчеркивается, что свобода коммуникаций в интернете не должна наносить ущерба человеческому достоинству, правам человека и основным свободам других лиц, особенно несовершеннолетних;
- в ней приветствуются усилия поставщиков услуг по сотрудничеству с правоохранительными органами в случаях размещения в интернете незаконного контента.

ВВУИО

На Всемирной встрече на высшем уровне по вопросам информационного общества были сформулированы следующие предложения для Партнерства по измерению ИКТ в целях развития с расчетом на то:

- что оно продолжит, расширит и углубит свою работу по измерению информационного общества, в том числе путем привлечения национальных статистических управлений как можно на более ранних этапах разработки статистических данных;
- что оно и впредь будет повышать осведомленность и создавать потенциал, уделяя особое внимание странам с низким уровнем доходов;
- что оно рассмотрит новые источники данных и методики;
- что оно создаст группу экспертов по целевым показателям ВВУИО.

Было достигнуто широкое согласие относительно необходимости продолжения процесса ВВУИО и мониторинга информационного общества после 2015 года при одновременном углублении характера такого мониторинга. Международное сотрудничество, а также национальная координация должны продолжаться, основываясь на модели, предполагающей участие многих заинтересованных сторон[152].

В Декларации о свободе в интернете активно отстаиваются интернет-свободы[153]. В преамбуле говорится, что свободный и открытый интернет может способствовать

---

152 *WSIS+10 High-Level Event 2014- Outcome Document: Forum Track*, http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/OutcomeDocument2014.pdf, последний раз обновлено 6 ноября 2014 года.

153 http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom, последний раз обновлено 8 августа 2014 года.

созданию лучшего мира[154]. В ней также поставлена цель убедить миллионы пользователей интернета поддержать эту Декларацию[155]. В Декларации поддерживается установление пяти основных принципов политики в отношении интернета:

- отказ от цензуры в интернете;
- всеобщий доступ к быстрым и приемлемым в ценовом отношении сетям;
- свобода подключения, общения, творчества и инноваций через интернет;
- защита новых технологий и их создателей от злоупотреблений со стороны пользователей;
- право на неприкосновенность частной жизни и возможность пользователей интернета защищать неприкосновенность своей частной жизни посредством контролируемого раскрытия информации о себе[156].

Проблемы в нормативной базе

А вот чего явно недостает, так это международного режима свободы в интернете, признаваемого всеми заинтересованными сторонами. Кроме того, свобода в интернете как явление поднимает различные правовые, политические и регуляторные вопросы, некоторые из них обсуждаются ниже.

Сегодня во многих юрисдикциях существуют основные права/национальные законодательные акты, гарантирующие свободу слова и выражения мнений в реальном мире. Эти же права также истолковываются как применимые к свободе слова и выражение мнений в интернете. Однако разоблачения Сноудена привлекли внимание к несанкционированным вмешательствам, нарушающим свободу слова и выражения мнений в интернете. Без ведома соответствующих пользователей за их сообщениями в виде аудио- и видеоматериалов, изображений или текста различными инстанциями ведется наблюдение. По сути, интернет и его различные объекты и платформы становятся средствами, обеспечивающими возможность создания общества, основанного на наблюдении. Из этого явствует, что в мире есть два типа людей – те, кто знает, что за ними ведется или велось наблюдение, и те, кто об этом не знает.

Рост наблюдения и мониторинга в интернете становится нормой и оказывает непосредственное воздействие на свободу слова и выражение мнений в интернете. Короче говоря, в то время как интернет не вполне представляет собой "дикий запад",

---

154 http://www.internetdeclaration.org/, последний раз обновлено 8 августа 2014 года.

155 Declaration of Internet Freedom, http://www.savetheinternet.com/internet-declaration.

156 http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom, последний раз обновлено 8 августа 2014 года.

из поступающих свидетельств также очевидно, что свобода слова в киберпространстве не является абсолютной свободой.

Нормы цивилизованного поведения в равной степени применимы к киберпространству. Это означает, что интернет-контент, направленный на то, чтобы порождать неудобства, неприязнь, ненависть, враждебность, или ориентированный на конкретное лицо или группу лиц, должен быть запрещен национальным законодательством.

Однако маска анонимности, предоставляемая интернетом, может внушить злонамеренным или склонным к злоупотреблениям пользователям чувство уверенности, что они могут безнаказанно говорить и делать что угодно.

Тем не менее на этом фоне в настоящее время формируется судебная практика в таких правовых режимах во всем мире, в соответствии с которой суды начинают сбрасывать эту завесу анонимности, предписывая поставщикам услуг раскрывать подлинную личность пользователей, занимающихся незаконной деятельностью. И все-таки, как уже указывалось, факт остается фактом – международного стандарта, определяющего свободу слова и выражения мнений в интернете, не существует.

Во Всеобщей декларации прав человека 1948 года содержатся некоторые основные принципы, которые можно считать полностью совместимыми с концепцией свободы в интернете.

Возникающие проблемы

Социальные сети принесли с собой новые виды онлайнового дискурса, которые свидетельствуют об умонастроениях людей. Между тем законы и законодательство во всем мире развиваются недостаточно быстро, чтобы решать возникающие проблемы, присущие социальным сетям.

Смартфоны и другие средства связи ознаменовали появление мобильного интернета. Сочетание мобильного телефона и интернета предоставляет неизвестные ранее возможности свободы слова в интернете. Проблема возникает в случаях, когда разные страны по-разному действуют в отношении ненадлежащего онлайнового контента, и связана с различиями в пределах понимания свободы слова в интернете в разных юрисдикциях. Несмотря на эти различия, существует всеобщее согласие в одной области, касающейся появления мобильного интернета, – сочетание мобильного телефона и интернета предоставляет неизвестные ранее возможности свободы слова в интернете.

Еще один обсуждавшийся ранее вопрос связан с возможностью свободного и анонимного общения в интернете. Как уже отмечалось, некоторые полагают, что анонимность в интернете позволяет им говорить там что угодно, не испытывая необходимости беспокоиться о возможном воздействии своих слов на других

людей[157]. Зачастую жертва предполагаемой клеветы в интернете подает иск против неустановленного ответчика.

В различных странах действуют разные законы о клевете, в которых идет речь о различных видах клеветнических высказываний или контента. Эти законы в равной степени применимы в киберпространстве. В этой связи в рамках формирующейся судебной практики становится все более ясно, что никто не имеет права порочить другого человека или пытаться нанести ущерб репутации других людей.

Положения национальных законов в разных странах в этом отношении различаются. Некоторые страны только ограничивают доступ к интернету, если считают, что это оправданно с точки зрения защиты моральных ценностей, личных юридических прав, интересов национальной обороны или государственной безопасности. Другие страны официально признали, что право на свободу выражения мнений распространяется на киберпространство, или рассматриваются возможность такого признания.

Все мы живем в переходный период в истории человечества, в который свободе в интернете угрожают не только государственные субъекты, но и частные, которые собственно управляют данными в интернете и контролируют их.

Другие проблемы, влияющие на свободу в интернете

Интернет-юрисдикция – одна из важных проблем, осложняемая тем, что свобода выражения мнений в интернете может ограничиваться в пределах территории той или иной страны, в то время как вы можете находиться физически в пределах юрисдикции другой страны. Кроме того, тот факт, что вы постоянно находитесь под прицелом киберпреступников, также может способствовать неполному осуществлению свобод в интернете. Таким образом, киберпреступность стала одной из важных правовых, политических и регуляторных проблем, которая потенциально может повлиять на свободу пользователей в интернете повсюду.

Еще одна проблема, влияющая на свободу в интернете, связана с кибербезопасностью. Пользоваться своей правовой свободой в интернете можно только в том случае, если он безопасен, защищен и надежен. Однако случаи нарушения кибербезопасности вновь выдвинули на передний план различные проблемы, возникающие в связи с обеспечением защиты и сохранности киберресурсов и инфраструктуры.

Свободу в интернете необходимо рассматривать совсем с другой точки зрения – с учетом глобального значения и уязвимостей этой киберсреды. В условиях быстрого роста кибератак на компьютерные системы и сети в различных странах потребуется

---

157 Eric Sinrod, *"Freedom of anonymous online speech has potential limits"*, http://www.lexology.com/library/detail.aspx?g=7a8eb382-b007-49c6-8ca1-4a9197062d9d, последний раз обновлено 8 августа 2014 года.

обеспечить баланс между свободой в интернете и необходимостью защиты и поддержания кибербезопасности.

Страны всего мира еще не пришли к единому мнению о том, как следует решать проблему ответственности информационного посредника. Некоторые страны, такие как США, не склонны возлагать такую ответственность на поставщиков услуг. Другие иногда предписывают посредникам проявлять должную исполнительность в случаях, когда они хотят избежать ответственности за потенциальное причинение ущерба третьим лицам в связи с онлайновыми данными при выполнении своих обязанностей, в отношении некоторых основных положений национального права.

Появление "темной паутины" (даркнета) является еще одним грозным вызовом для свободы в интернете. Киберпреступники без колебаний пользуются этой зоной для осуществления своих злонамеренных планов и действий, направленных на ущемление реализации людьми свободы в интернете.

Другой серьезный вызов для доверия при использовании киберпространства и свободы в интернете – это растущий феномен кибервойны, что сегодня ни для кого не является секретом. Возникновение кибертерроризма на практике еще более влияет на полноту осуществления свобод в интернете.

Несомненно, в контексте свободы в интернете существует необходимость в международном взаимопонимании и принципах общего знаменателя. По важным правовым и политическим вопросам, влияющим на упоминаемую выше свободу в интернете, проделана большая работа. Именно в этом контексте такие организации как Всемирная федерация ученых и Международный союз электросвязи могут и далее играть важную роль в содействии достижению формирующегося консенсуса в отношении дальнейших действий.

Большие данные

На этом этапе не следует упускать из виду воздействие больших данных на свободу в интернете, поскольку, в конечном счете, эту свободу необходимо рассматривать в контексте электронных данных и информации. Сегодня интернет представляет собой гигантскую сеть сетей – огромное хранилище данных бесконечной емкости. Поэтому необходимо также учитывать, что между свободой в интернете во всех ее формах и большими данными существуют непосредственная связь, взаимодействие и взаимозависимость.

Большие данные – важная реалия нашего времени. При таком большом объеме данных, генерируемых различными компьютерными системами и сетями, вполне естественно, что компании захотят заниматься анализом больших данных. Большие данные по-разному определяются различными заинтересованными сторонами и представляют также важную правовую, политическую и регуляторную проблему.

Определение термина "большие данные"

В **Википедии** дается следующее определение больших данных: "[…] всеобъемлющий термин, относящийся к любому набору данных настолько большому и сложному, что данные становится затруднительно обрабатывать с использованием имеющихся инструментов управления данными или традиционных приложений для обработки данных. Однако большие данные, как правило, включают массивы данных, размер которых превосходит возможности обычно используемых программных средств по вводу, отбору для хранения, управлению и обработке информации в пределах допустимых затрат времени"[158]. В **Оксфордском словаре** термин "большие данные" определяется так: наборы данных, которые слишком велики и сложны, для того чтобы с ними можно было работать или формировать запросы с использованием стандартных методов и средств[159]. В **докладе Белого дома о больших данных**, опубликованном 1 мая 2014 года, повторяется широко принятое в настоящее время определение, согласно которому большие данные "настолько велики по объему, настолько разнообразны или перемещаются с такой скоростью, что традиционных способов сбора данных недостаточно"[160]. Ассоциация **TechAmerica Foundation** указывает: "Большие данные – это термин, относящийся к огромным объемам высокоскоростных, сложных и переменных данных, которые требуют передовых методов и технологий для сбора, хранения, распределения, управления и анализа информации"[161].

Для больших данных характерно, в частности, следующее:

- они должны быть эластичными по характеру[162];
- во многие системы больших данных поступают необработанные данные, а это значит, что всегда имеются элементы данных, характеризующиеся чрезвычайно резко отклоняющимися значениями, из-за чего в системе появляются критические участки;
- большие данные могут быстро получать запрашиваемые циклы вычислений посредством использования облачной инфраструктуры как услуги[163];

---

158 http://en.wikipedia.org/wiki/Big_data

159 http://www.oxforddictionaries.com/definition/english/big-data

160 http://www.lexology.com/library/detail.aspx?g=e7161021-7570-476c-bf8a-b4637d10a355

161 TechAmerica Foundation, Demystifying Big Data: A Practical Guide to Transforming the Business of Government 2012, https://www-304.ibm.com/industries/publicsector/fileserve?contentid=239170, последний раз обновлено 4 августа 2014 года.

162 http://hadoopblog.blogspot.in/2012/02/salient-features-for-bigdata-benchmark.html

163 http://www.dummies.com/how-to/content/characteristics-of-big-data-analysis.html

- в этом контексте очень важен объем генерируемых данных. Именно объем данных определяет их ценность и потенциал, а также то, могут ли они действительно считаться большими данными;
- разнообразие предполагает необходимость справляться со сложностями, связанными с наличием данных разных типов, включая структурированные, полуструктурированные и неструктурированные данные;
- скорость генерирования, обработки и анализа данных продолжает расти. Ее росту способствует протекающее в режиме реального времени генерирование данных, а также необходимость использования в бизнес-процессах и при принятии решений потоковых данных;
- неопределенность данных – достоверность означает уровень надежности, связанный с определенными видами данных[164].

С большими данными связано много правовых, политических и регуляторных проблем. Прежде всего следует отметить, что в сфере больших данных не существует каких-либо международных рамок или международных договоров. В силу этого большие данные относятся к тем вопросам, которые продолжают регулироваться национальными законами. Дело же обстоит так, что в большинстве стран нет специального законодательства или правовых положений в этом отношении. Однако в целях обеспечения политических и регуляторных рамок крайне необходимо учитывать упомянутые ниже важные параметры.

Одной из крупнейших проблем в области больших данных является защита данных. В различных национальных юрисдикциях предусмотрены разные регуляторные требования в отношении защиты данных. В Европейском союзе имеются директивы о защите данных, а страны других регионов включили различные положения о защите данных в соответствующее национальное законодательство. Важное значение имеют методы сбора, защиты и сохранения данных. К вопросу о защите больших данных явно необходимо вновь вернуться, поскольку законодательство о защите данных всегда разрабатывалось для относительно небольших объемов данных, которые генерируются отдельными лицами и которые ничтожно малы по сравнению с объемами больших данных.

Защита больших данных связана с колоссальными проблемами как для тех, кто их обрабатывает, так и для регуляторных органов. Их огромный объем и архитектура ссылок и разнообразных источников требуют четкой безопасной и защищенной правовой базы, которая способствует защите как пользователей, так и поставщиков данных.

---

164 IBM, Analytics: The real-world use of big data- How innovative enterprises extract value from uncertain data, http://www.ibm.com/smarterplanet/global/files/se__sv_se__intelligence__Analytics_-_The_real-world_use_of_big_data.pdf, последний раз обновлено 8 августа 2014 года.

Минимизация данных также порождает вопросы о конфиденциальности и защите данных. Особое значение имеет необходимость определения надлежащего международного передового опыта в области сбора, хранения и уничтожения данных, в том числе персональных данных в форме, позволяющей идентифицировать субъекта этих данных.

В национальных законодательствах вопрос об индивидуальном согласии на сбор, использование или раскрытие данных, в противоположность индивидуальному контролю данных, трактуется по-разному. А как уже упоминалось, какого-либо охватывающего большие данные международно-правового механизма по этому и другим относящимся к киберпространству вопросам не существует.

Еще один правовой вопрос связан с анонимностью данных и маскированием данных для лиц, размещающих информацию в интернете. Одни из не решенных должным образом важных вопросов касается основных принципов, которые должны применяться в контексте сбора, обработки, хранения и распространения больших данных. С учетом того факта, что большие данные сегодня неизменно размещаются в облачной среде, их защита и сохранение представляют новые правовые, политические и регуляторные проблемы.

Конфиденциальность данных является одним из важных вопросов, связанных с большими данными, вследствие огромных объемов потребляемых данных, а также из-за того, что каждый поставщик данных имеет неотъемлемое право на защиту и сохранение своих данных. Поэтому ответственность за обеспечение надлежащей защиты этих данных лежит непосредственно на сетевой службе.

Кроме того, одним из важных правовых, политических и регуляторных вопросов является юрисдикция, к которой относятся большие данные, поскольку такие данные неизменно находятся в облаке и на других различных серверах, размещенных в разных частях мира. В случаях нарушения конфиденциальности больших данных заинтересованное лицо должно предъявлять иск соответствующим поставщикам услуг. Большой проблемой будет определение физического местонахождения указанных данных, поскольку последствия установления местоположения сервера, где произошло нарушение, будут зависеть от местных законов о нарушении конфиденциальности.

Киберпреступность, связанная с большими данными, также является одной из значительных правовых проблем, поскольку вся экономика интернета основывается на этих данных, и несанкционированные нарушения конфиденциальности больших данных могут в значительной мере помогать киберпреступникам; именно поэтому они склонны все чаще действовать в этой сфере.

В октябре 2013 года компания Adobe подтвердила, что киберпреступники незаконно получили доступ к ее сети, завладев сведениями об именах более чем 2,9 миллиона пользователей, зашифрованных номерах кредитных и дебетовых карт, датах

истечения срока действия карт, идентификационных данных для регистрации и паролях. Был также получен доступ к исходному коду нескольких продуктов компании Adobe, включая Acrobat и ColdFusion[165].

Европейское агентство по сетевой и информационной безопасности (ENISA), являющееся консультативным органом ЕС, заявило в январе 2013 года: "Использование больших данных затронет конфиденциальность данных. В то же время использование больших данных через злоумышленников может открыть путь для векторов атак нового вида"[166]. ENISA также указало, что большие данные представляют собой массив информации, генерируемой "в результате быстрого распространения социальных технологий, облачных вычислений, мобильных вычислений и использования интернета в целом", и что они стали одной из новых проблем безопасности.

Конфиденциальность

Аналитика больших данных может оказать непосредственное влияние на нарушение неприкосновенности частной жизни. В мае 2014 года Белый дом выпустил долгожданный доклад, посвященный большим данным под названием "Big Data: Seizing Opportunities, Preserving Values" (Большие данные: использование возможностей, сохраняя ценности). Доклад был подготовлен по просьбе президента Барака Обамы, и в нем рассматриваются пути быстрого роста технических достижений, которые позволяют как правительствам, так и частному сектору осуществлять сбор, хранение, анализ и использование огромных объемов больших данных. В нем освещаются потенциальные угрозы неприкосновенности частной жизни и равенству, которые могут порождаться большими данными сейчас и в будущем, а также поддерживаются правовые, политические и регуляторные инициативы по защите граждан в США и во всем мире от потенциальных злоупотреблений[167].

Таким образом, большие данные и конфиденциальность данных приобретают все большее значение в мире права. Будут часто возникать споры по поводу того, кому принадлежит контент больших данных, особенно тогда, когда в разработке систем, предназначенных для их генерирования, принимают участие третьи стороны. Еще

---

165 http://blogs.mcafee.com/consumer/consumer-threat-notices/malicious-acrobatics-adobe-the-latest-target-in-string-of-cyber-attacks

166 http://www.out-law.com/en/articles/2013/january/cloud-mobile-social-and-big-data-technology-innovations-increasing-threat-of-cyber-attacks-says-eu-body/

167 Kenneth R. Florin, Ieuan Jolly et. al. "White House "big data" report highlights benefits and potential for abuses from big data", http://www.lexology.com/library/detail.aspx?g=a036aed0-cffb-4ae1-a518-44b92201effb, последний раз обновлено 4 августа 2014 года.

одной серьезной проблемой является защита данных, включая конфиденциальную личную информацию, с помощью криптографии и детального управления доступом.

Поиск и извлечение больших данных и доступ к ним также неразрывно связаны с конфиденциальностью и являются главными правовыми проблемами в контексте сохранения полученных данных и анализа данных. Первостепенное значение имеет поддержание аутентичности, целостности и достоверности больших данных, к которым осуществляется доступ, и извлеченных больших данных.

Кроме того, использование усиленной с помощью криптографии защиты, ориентированной на данные, порождает собственные правовые проблемы. В дополнение к этому детальное управление доступом влечет за собой некоторые другие сложные правовые и политические проблемы, касающиеся конфиденциальности. К тому же существует необходимость защищать конфиденциальность при распространении информации.

Еще одной проблемой, связанной с большими данными, является то, что когда данные собраны, сохранять их анонимность становится очень сложно. Одновременно с осуществлением многообещающих проектов по исследованию способов сохранения в тайне идентифицирующей личность информации при работе с большими массивами данных в настоящее время предпринимаются более продвинувшиеся вперед усилия по повторной идентификации якобы "анонимных" данных. Совокупные инвестиции в возможность слияния данных в разы больше вложений в технологии по повышению конфиденциальности[168]. Одной из первостепенных проблем является обеспечение аутентичности, целостности и достоверности больших данных, предназначенных для доступа и поиска и извлечения.

Другие правовые проблемы связаны с обеспечением безопасности инфраструктуры больших данных в виде наличия надлежащей правовой базы для защиты вычислений в структурах распределенного программирования. В связи с этим необходимо определить надлежащий передовой опыт обеспечения и поддержания безопасности нереляционных хранилищ данных. Еще одна важная правовая проблема касается управления данными. В этой связи необходимы надлежащая нормативно-правовая база для защиты хранилищ данных и журналов транзакций, а также детальных проверок.

Права интеллектуальной собственности на большие данные – еще один важный правовой вопрос. Кому принадлежат права интеллектуальной собственности на большие данные? Каковы права интеллектуальной собственности, связанные со сбором, хранением, обработкой или совместным использованием больших данных?

---

168 Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values,* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf, последний раз обновлено 4 августа 2014 года.

Часто высказываются опасения, что новые инструментальные средства поиска и анализа больших данных могут привести к нарушению авторских прав на данные. Другие опасения связаны с определением ответственности соответствующих договаривающихся сторон за неточную или неполную информацию и в случаях несоблюдения договорных соглашений.

Не исключено также, что технологии открывают возможность несанкционированного доступа к информации о деловых конкурентах, вызывая различные проблемы с точки зрения конкурентного права. Факт зависимости прибыльности больших данных от таких коммерческих тайн и конфиденциальных персональных данных сам по себе оказывает воздействие на действительную конфиденциальность и безопасность и подрывает доверие к использованию киберплатформ и технологий.

Утверждается, что сбор и обработка больших данных оказывают влияние на индивидуальную и коллективную идентичность людей, что угрожает снижением качества демократии.

Еще одна проблема связана с тем фактом, что многие цензоры больших данных являются в основном влиятельными посредниками, в результате чего увеличивается риск неправомерного использования таких данных и злоупотребления ими, что приводит к нарушению прав личности и свобод людей.

Говоря коротко, существует необходимость предложить соответствующую нормативно-правовую базу для обеспечения того, чтобы большие данные никоим образом не наносили ущерба осуществлению прав граждан или, более того, выполнению ими их гражданских обязательств и обязанностей.

Роль Всемирной федерации ученых и МСЭ

С учетом отсутствия международных параметров, относящихся к правовым и политическим рамкам для больших данных, крайне необходимо, чтобы такие организации как Всемирная федерация ученых и Международный союз электросвязи продолжали усилия по содействию ее разработке.

Заключение

В заключение можно констатировать, что как свободы в интернете, так и большие данные являются представляющими острый интерес развивающимися концепциями, которые играют все более значительную роль в нашей повседневной жизни. Поэтому крайне важно разработать и внедрить надлежащие международные правовые, политические и регуляторные рамки для сохранения свободы в интернете. На карту поставлено само будущее этих структур цифровой эпохи, которые столь хорошо нам служат и от которых мы стали столь зависимыми в очень многих отношениях.

Перед нами стоит важная задача – разработать и внедрить такие международные политические и регуляторные рамки, основанные на общепризнанных принципах.

Эти рамки со временем будут неизбежно развиваться. В настоящее время реализуется много инициатив в области судебной практики, касающихся свободы в интернете и больших данных. Однако крайне важно, чтобы предпринимались усилия в целях обеспечения разработки эффективных политических и регуляторных рамок на международном уровне.

Постоянная группа по мониторингу информационной безопасности Всемирной федерации ученых может сыграть чрезвычайно важную роль в этом отношении, не только выполняя мониторинговые функции, но и внося свой вклад в формирование таких международных рамок. Хочется надеяться, что Всемирная федерация и другие соответствующие организации вместе с Международным союзом электросвязи смогут внести значительный вклад в достижение этой цели, соразмерный их знаниям и опыту в данных областях. Если бы эти организации смогли помочь разработать общепризнанные принципы общего знаменателя, направленные на обеспечение надлежащей среды киберпространства, это, несомненно, принесло бы большую пользу всем заинтересованным сторонам.

Как уже упоминалось, на карту поставлена имеющаяся у всех пользователей возможность продолжать пользоваться преимуществами свободы в интернете путем преодоления проблем кибербезопасности и других проблем, которые угрожают подорвать доверие к этой растущей и все более незаменимой вселенной.

Можно надеяться на то, что по мере увеличения числа пользователей интернета и ускорения прогресса в области кибертехнологий будет развиваться соответствующая судебная практика. Только постоянно следя за изменениями в судебной практике и способствуя прогрессу в этом отношении, мир в целом и ключевые игроки в частности смогут определить дальнейшие шаги.

Процесс формирования соответствующих правовых, политических и регуляторных рамок для больших данных и свободы в интернете будет развиваться со временем. Одной из важных предпосылок успеха в этой сфере будет распространение уважения к основным правам на киберпространство.

3.3 Наблюдение со стороны государства в киберпространстве с глобальной точки зрения

Говард Шмидт

Введение

Для того чтобы составить правильное представление о наблюдении в киберпространстве и высказать взвешенное мнение по этому вопросу, важно сначала понять, что наша система ориентиров сложилась в основном в мире, в котором правила взаимодействия (писаные или иные) формировались постепенно,

в частности в период задолго до появления того, что мы называем киберпространством.

На каждого человека, считающего наблюдение оправданным, всегда находится кто-то, придерживающийся противоположной точки зрения, а также огромное число заинтересованных лиц, не имеющих четкого мнения по этому вопросу. Именно на основе изучения фактической информации и осмысления ситуации с глобальной точки зрения мы сможем в конечном счете предложить сбалансированный комплекс руководящих принципов, которые могут учитывать все заинтересованные стороны при определении как целесообразности, так и оправданности наблюдения со стороны государства.

Сбор данных

Рост технологий привел к появлению среды, в которой с различными целями генерируются, передаются и собираются огромные объемы данных. Все, что создается в киберпространстве, создается из данных, и непременным условием является фиксация этих данных, а также сбор зафиксированных данных. Примерами важных данных, которые должны фиксироваться и собираться, являются данные о финансовых транзакциях. Рассмотрим, если угодно, современный платежный чек. Многие из нас получают вознаграждение за труд в виде электронного перевода средств, которые размещаются на наших счетах, и многие собирают и хранят эти электронные данные в виде сберегательного счета. Эти хранимые данные могут быть перемещены в другую точку сбора данных в виде транзакции (например, в продовольственном магазине), в рамках которой товары обмениваются на данные, выступающие в роли финансового инструмента.

Еще одним примером сбора данных подобным образом является разговор по мобильному телефону между двумя сторонами, при котором компания подвижной телефонной связи отслеживает, куда звонили, когда звонили и как долго длился разговор. Это делается в целях выставления счетов, как объясняет нам как потребителям телефонная компания. Веб-сайты собирают данные о пользователях веб-сайта и услуг в различных целях, в том числе в целях установки и сохранения предпочтений пользователя и хранения информации, генерируемой пользователем (например, на веб-сайте социальной сети).

Как граждане в киберпространстве мы все понимаем и признаем, что существуют обстоятельства, в которых сбор данных не только обоснован и приемлем, но и во многих случаях желателен. Чем определяется принятие факта сбора данных заинтересованными сторонами, так это четким пониманием того, какие данные собираются и для какой цели. В таких случаях мы решаем принять условия, на которых осуществляется сбор данных, до начала соответствующей деятельности или решаем отказаться от участия в ней, если считаем политику сбора и использования данных слишком обременительной.

В сущности, как заинтересованные стороны мы все согласны на заключение с теми, кто имеет доступ к нашим данным, соглашения, в котором четко определено, как могут собираться и использоваться наши данные, кто может хранить данные (например, компания сотовой связи) и в какой степени ответственность за хранение может быть передана и кому. Хранители данных обладают огромной властью над ними, однако это не дает им права поступать с данными так, как они считают нужным. В конечном счете, как только хранитель данных решает использовать их не так, как предусмотрено в соглашении с лицом или организацией, к которым относятся данные, он/она должны заключить новое соглашение, разрешающее такое расширенное использование данных. В противном случае это может обоснованно истолковываться как злоупотребление полномочиями или нарушение доверия.

Судебный процесс и сбор разведывательной информации

Именно по вышеупомянутым причинам сегодня существуют процессы, позволяющие расширенное использование данных, которое выходит за рамки ожиданий соответствующих заинтересованных сторон. При наличии обоснованного подозрения, что кто-то занимается преступной деятельностью, есть правовые и судебные процессы, позволяющие вести контроль и получать доступ к собранным данным, которые могут быть использованы как доказательство противоправных действий. Правила и процедуры, связанные с этим видом наблюдения, во всем мире различны, однако у населения в целом обычно есть доступ к правилам взаимодействия.

Некоторая неопределенность возникает в ситуациях, когда наблюдение ведется государственными разведывательными службами. На глобальном уровне разведывательные службы тайно осуществляют мониторинг и сбор данных, а также используют информацию в различных целях. Очевидно, большинство служб будут утверждать, что собранная информация служит делу национальной безопасности (как, например, в случае недавних публичных заявлений АНБ) или всеобщего блага. Другие могут просто заявлять, что в силу своих суверенных полномочий они могут поступать таким образом и что они, в сущности, не должны объяснять, почему занимаются сбором разведывательной информации. Дело особенно осложняется в условиях глобальной экономики, когда две или несколько стран занимают различные позиции по вопросу сбора таких данных. В таких случаях киберграждане могут полагать, что им обеспечивается определенный уровень конфиденциальности в соответствии с правилами, установленными их правительством, однако они передают информацию в киберпространстве, в котором пути перемещения данных от источника до конечного получателя могут пересекать национальные границы. Как только данные оказываются в месте, где действуют иные правила, они подпадают под действие этих правил. Поскольку сбор разведывательных данных представляет собой закрытый процесс, на который, как правило, не распространяются требования транспарентности, предусмотренные правоохранительными и судебными процедурами, становится крайне трудно определить, когда переходится та или иная грань.

Методы и правила сбора разведывательной информации

При наличии разрешения на сбор разведывательной информации за рамками правовой или судебной процедуры (а во многих случаях именно так и есть) важно принимать во внимание использование разведывательными службами вредоносных программ и скрытно размещаемых приложений. Во многих суверенных государствах создание вредоносных программ и приложений, предназначенных для проникновения в компьютерные системы с использованием различных способов распространения, само по себе является абсолютно незаконным. Любая деятельность, выполняемая вредоносными программами после их распространения, также рассматривается как преступная деятельность их создателя, равно как и любого пользователя или организации, осознанно распространяющих и использующих вредоносные программы для осуществления такой деятельности. Правовые и судебные процедуры, установленные в глобальном масштабе, в настоящее время распространяются на такую деятельность, и наказание за нарушение закона в этой связи может быть весьма суровым.

И в этом случае, когда речь идет о методах работы разведывательных служб, финансируемых государством, правила осуществления деятельности, связанной с созданием и распространением вредоносных программ и скрытых приложений, и сбора данных с помощью таких "инструментов" являются весьма неопределенными. В зависимости от конкретного рассматриваемого суверенного государства ведение такой деятельности государственной разведывательной организацией может считаться приемлемым по разным причинам – вероятно, чаще всего по соображениям национальной безопасности. Однако важно отметить, что после размещения вредоносная программа может распространиться (что часто и происходит) далеко за предусмотренные границы и оказать негативное воздействие на системы, которые, по всеобщему признанию, должны быть вне сферы интереса служб, занимающихся сбором разведывательной информации. В качестве примера можно назвать такие особо важные системы, как больничные сети, энергетические системы и системы безопасности, применяемые для управления опасными процессами (например, химическим производством). Кроме того, возможно негативное воздействие на финансовые системы, системы производства продуктов питания и системы предприятий обрабатывающей промышленности, что может породить лавину волнений и паники в обществе.

Выравнивание игрового поля для кибероружия

Описанное здесь применение вредоносных программ можно рассматривать как эквивалент применения кибероружия в том понимании, что оружие может оказывать воздействие отнюдь не только на намеченную цель. Кроме того, возможность создавать и развертывать кибероружие не ограничивается никакой нехваткой экономических и природных ресурсов, которая, как правило, встречается при традиционных физических конфликтах. Наличие металлов, химических объектов или

высокотехнологических средств мало сказывается на возможностях создателей вредоносных программ. Компьютера с подключением к сети или внешнего носителя информации для хранения и транспортировки (например, карты памяти USB) более чем достаточно при наличии знания о том, как создавать вредоносные программы.

После того как вредоносная программа создана и распространена, она может быть превращена в оружие и использована любым лицом или организацией, которые смогут выявить и выделить ее. А это значит, что кибероружие может быть обращено против создавшей его организации, возможно, в видоизмененной версии с улучшенной функциональностью по сравнению с исходным пакетом вредоносных программ. В таких случаях организация, внедрившая вредоносную программу, изначально выступает в роли глобального поставщика кибероружия. Это, по сути, означает, что, если не считать получаемых в результате первого удара преимуществ, игровое поле вскоре после внедрения программы выравнивается для всех сторон, что может привести к возникновению крайне деструктивной среды, в которой ни один человек и ни одна организация не смогут найти укрытия. Кроме того, кибероружие, будучи развернуто, по сути, существует вечно, поскольку нет запасов, которые можно уничтожить.

Дальнейшие шаги

Совершенно очевидно, что независимо от намерений тех, кто осуществляет финансируемое государством скрытое наблюдение, возникают сопутствующие проблемы, которые могут привести к потенциально не поддающимся контролю и непредвиденным негативным последствиям. Это может повлечь за собой цепную реакцию, которая может потенциально дестабилизировать глобальные отношения и экономическую ситуацию. Хотя интернет может служить эффективным средством ведения наблюдения с намерениями, которые кто-то может считать благими, важно понимать, что он стал неотъемлемой и необходимой частью мировой экономики, позволяя отдельным лицам, организациям и странам всех размеров на равных принимать в ней участие. Интернет также обеспечивает условия для мгновенного свободного обмена идеями и для сотрудничества на каждом уровне экономической иерархии.

Поэтому важно, чтобы глобальное деловое сообщество на всех уровнях повсюду оказывало давление на правительства, с тем чтобы они принимали соответствующие законы. Такие законы должны способствовать предотвращению возможного подрыва экономических и социальных преимуществ, обеспечиваемых интернетом. Они должны также обеспечивать возможность для постоянного роста числа отдельных лиц, организаций и стран, которые могут участвовать в совместной экономике, стимулируемой стабильным интернетом, в котором каждый может сохранять уверенность, зная, что интересы правительства не ставятся выше интересов народа, которому оно служит.

3.4 Масштабы наблюдения со стороны государства в киберпространстве: точка зрения Европейского союза

Хеннинг Вегенер

Неизбежное и растущее внутреннее противоречие между свободой и целостностью интернета (и цифровой связи в целом), с одной стороны, и, с другой стороны, все более настоятельными потребностями в общественном порядке и проблемами коллективной безопасности в полной мере отражено во многих разделах данной публикации, особенно в работе проф. Аль-Ашкара, посвященной свободам в интернете и гражданским свободам в сети.

В условиях очевидных всем в настоящее время масштабных несанкционированных проникновений в цифровые устройства и сети и панического страха перед большими данными это противоречие сейчас как никогда занимает видное место среди широко распространенных опасений населения в Европе. Небывалый рост технических возможностей сбора и обработки данных, который выводит человечество в новую эпоху, характеризующуюся утратой неприкосновенности частной жизни, породил опасения, что принципы национального и международного права и личное и коллективное имущество подвергаются серьезной угрозе. Все более широкие посягательства на основные права человека обоснованно стали глобальной проблемой, и определение правил и пределов этой на первый взгляд неудержимой волны требует принятия мер по исправлению ситуации на глобальном уровне.

Важное начало формированию необходимой политики было положено резолюцией A/RES/68/167 Генеральной Ассамблеи ООН "Право на неприкосновенность личной жизни в цифровой век", принятой без голосования 18 декабря 2013 года, в которой выражается готовность международного сообщества противодействовать массовому слежению, перехвату и сбору личных данных. Во исполнение пункта 5 постановляющей части этой резолюции Верховный комиссар ООН по правам человека в июне 2014 года представил доклад (A/HRC/27/37), который был обсужден Советом по правам человека в ходе групповой дискуссии, состоявшейся в сентябре на его 27-й сессии, и, как ожидается, будет обсуждаться ГА ООН на ее текущей 69-й сессии "с мнениями и рекомендациями", которые должны быть рассмотрены государствами-членами. В этом докладе четко изложены требования в области прав человека, предъявляемые к мерам по наблюдению со стороны государства – они должны быть необходимыми и соразмерными, прозрачными и обеспечивать уважение прав лиц на неприкосновенность частной жизни за границей. Докладчик ясно показывает, что, по его мнению, эти требования в настоящее время не выполняются.

Пока не достигнуты конкретные результаты этой глобальной работы, несмотря на всеобщие потребности и подходы, существуют впечатляющие региональные различия в том, как страны и население реагируют на разоблачения и факты

нарушений неприкосновенности частной жизни в цифровой среде, нарушений национального суверенитета и нарушений в области защиты информации (в рамках широкой общественной дискуссии, вызванной делом Сноудена).

В некоторых частях мира наблюдается скорее смирение, чем протест или даже безразличие; во многих крупных странах публично высказываемое несогласие приглушается существующими политическими системами; в США существует намного более глубокое понимание предполагаемых или реальных потребностей общественной безопасности, поддерживаемое более гибкой правовой системой. В Европе, и главным образом в Европейском союзе, с другой стороны, разоблачения и сами масштабы незаконной кражи данных вызвали сильнейшее смятение и несогласие. Возникло широкое политическое движение, которое легкомысленно было бы недооценивать, в особенности в его трансатлантических аспектах коллективной утраты доверия – кибердоверия, так сказать. Это не могло не затронуть многолетнюю тесную связь европейских демократий с США, подкрепляемую сильной эмоциональной привязанностью.

Это коллективное настроение в Европе отражает ее страстное стремление к свободе и неприкосновенности частной жизни, которое, несомненно, во многом усиливается под влиянием ее недавней истории, ознаменованной диктаторскими режимами и свойственным им отрицанием неприкосновенности частной жизни (которые все еще живы в памяти), а также вследствие высокого уровня развития в ней защиты данных и гражданских свобод и самой природы Европейского союза как субъекта права. Страх перед всемогущим Большим братом – левиафаном, не ограничиваемым никакими законами, распространен в Европе в гораздо большей степени, чем где-либо еще, хотя было бы неправильным недооценивать и коллективное беспокойство американцев в связи с масштабным слежением со стороны правительства. Этот неоднозначный вопрос будет, вероятно, играть важную роль на следующих президентских выборах.

Однако если мы стремимся определить глобальные критерии для поддержания кибердоверия в эру, предоставляющую безграничные технические возможности для несанкционированного проникновения, может быть желательно рассмотреть ситуацию в ЕС и его правовую среду, поскольку это может помочь обеспечить важный компонент всеобщей нормативной базы.

Один из аргументов в пользу этого заключается в том, что ЕС представляет собой основанное на праве сообщество, в состав которого входит 28 промышленно развитых стран, играющих важную роль в мировой цифровой экономике, в которых цифровые технологии более чем где-либо стали парадигмой экономики и общества; до сих пор ЕС является крупнейшим экономическим блоком мира. Из-за этого страны ЕС соответственно подвергаются большей угрозе кибератак, чем многие другие страны; компания McAfee определила, что Германии, например, с ущербом от кибератак в размере 1,65% ее ВНП, принадлежит рекорд среди промышленно развитых стран. В то время, когда одним из основных факторов, способствующих нанесению ущерба

странам с открытой экономикой, сильно зависящей от интернета, стали сообщества киберпреступников и когда для иностранных разведслужб наступило раздолье, киберпреступность в Европе стала суровой реальностью. Это побудило Европейский союз к разработке высокоразвитой единой системы коллективной кибербезопасности.

ЕС одновременно представляет собой объединение 28 независимых стран и организацию с едиными институтами и нормоустанавливающими органами. Большинство законодательных актов являются результатом совместных решений Европейского совета – по инициативе Комиссии ЕС – и Европейского парламента. Резолюции и решения незамедлительно становятся обязательными для всех государств-членов во всех их частях в соответствии с директивами о достижении согласованных целей. Эти резолюции и решения должны быть транспонированы в национальные законы государств-членов, что является уникальной особенностью данной международной системы. Благодаря единой институциональной основе европейское законодательство не только обеспечивает незамедлительный правовой эффект в государствах-членах, но и оказывает воздействие на другие страны мира. Таким образом, ЕС может стать примером, который многие могут счесть достойным подражания, в качестве институциональной лаборатории, в которой большая группа стран апробирует то, что может быть также внедрено международным сообществом в целом. Законодательство ЕС является мощным инструментом внутренней координации и гармонизации, а также путем к международному регулированию.

Как кибербезопасность, так и политика гарантирования защиты персональных данных относятся к компетенции европейских органов. Что касается кибербезопасности, Европейская комиссия более 10 лет работает над созданием нормативной базы для своих государств-членов. Ряд важных документов, отчасти аналитических и отчасти директивных, образовали всеобъемлющий свод норм права, обязательный для государств – членов ЕС, который как по объему, так и по степени детализации не имеет аналогов в цифровом мире стран, за исключением США. Кроме того, в 2004 году 28 государств-членов создали Европейское агентство по сетевой и информационной безопасности (ENISA) в качестве объединенного аналитического центра – координатора важной совместной деятельности ЕС и органа, стимулирующего дальнейшие регуляторные меры. Следует упомянуть также Европейский центр по борьбе с киберпреступностью при Европоле и общеевропейскую CERT в качестве центрального пункта для контактов и принятия решений в случае кибератак. Здесь нет возможности описать весь спектр деятельности ЕС по борьбе с киберпреступностью в правовом и институциональном аспектах, но общее представление можно легко

составить по веб-странице ENISA и другим доступным аналитическим материалам[169]. ЕС твердо придерживается своей Цифровой повестки дня и курса на оптимизацию стратегии кибербезопасности. Двумя недавно опубликованными всеобъемлющими документами, включающими ранее принятые нормы, заслуживающие изучения, являются Стратегия кибербезопасности Европейского союза[170] (2013 год) и проект Директивы по сетевой и информационной безопасности[171] (NIS). Оба документа, но особенно Директива по NIS, устанавливают всеобъемлющие требования, стандарты и обязательства для частного сектора, групп CERT, операторов ключевых объектов инфраструктуры, сетей и информационных систем.

Особый интерес в нашем контексте представляет то, что ЕС образует территорию унифицированного киберправа. 23 страны из 28 инкорпорировали Будапештскую конвенцию о киберпреступности в национальное законодательство (остальные, несомненно, сделают это в ближайшее время), и все из них инкорпорировали (аналогичную) Директиву 2002 года[172]. Таким образом, во всех странах киберпреступления и любое несанкционированное проникновение в цифровые устройства и сети являются в равной степени наказуемыми, а правоохранительная деятельность может осуществляться в любом месте Союза.

Еще одним важным аспектом цифровой политики ЕС является защита данных. Вопросы защиты личной информации и частная сфера жизни людей приобрели значение только с развитием хранения цифровых данных. Применимые законы ЕС имеют большие перспективы. Правовой базой в настоящее время по-прежнему является Директива 95/46EG ЕС, в которой излагаются минимальные стандарты защиты, инкорпорированные всеми членами ЕС в свое национальное законодательство. Директива применяется в отношении персональных данных частных лиц. Использование данных является законным, если соответствующее лицо дало на это согласие или если возникли другие строго определенные обстоятельства.

---

169 www.enisa.europa.eu. См. также Henning Wegener, *La ciberseguridad en la Unión Europea,* www.iees.es/Galerias/fichero/docs_opinion/DIEEE077bis-2014_CiberseguridadProteccionInformación_H.Wegener.pdf. Вариант статьи на немецком языке размещен по адресу www.unibw.de/infosecur.

170 JOIN (2013)1 final.

171 COM (2013)48 final.

172 COM (2002)173 final.

Эти ограничения также в некоторой степени относятся к пользователям данных, которые находятся за пределами Союза[173].

В 2010 году Комиссия ЕС приступила к осуществлению более амбициозного законодательного проекта в целях адаптации практикуемой в настоящее время защиты данных к изменившимся обстоятельствам[174]. В проекте регламента – Генерального регламента по защите данных (GDPR) – предпринята попытка зафиксировать потребности развитого информационного общества, которое характеризуется значительно возросшими потоками данных, облачным хранением, новыми социальными сетями и экспоненциальным ростом возможностей подключения. В качестве регламента новый документ сразу после его принятия станет обязательным во всех государствах-членах и будет представлять собой единый свод норм ЕС, включая подробный единый набор правил для всех 28 членов. Регламент является более строгим и подробным документом, чем Директива 1995 года, и предусматривает крупные штрафы в случае нарушения. Проект документа прошел через Европейский парламент в марте 2014 года и в настоящее время обсуждается правительствами в целях принятия решения в Европейском совете. Ожидается, что он будет принят в окончательном виде в ближайшие несколько месяцев, а затем вступит в силу в 2016 году. Однако он уже оказывает упреждающее воздействие, поскольку показывает, что ЕС движется в направлении очень жесткого режима защиты данных.

После этого краткого общего обзора действующего и будущего европейского законодательства как цельной правовой структуры можно вернуться к вопросу наблюдения в киберпространстве. Любое несанкционированное проникновение в носители цифровых данных – компьютеры, телефоны, сети, другие цифровые устройства – и копирование, хищение, изменение или передача хранимых данных в случае отсутствия особых оснований для этого являются киберпреступлениями. Если имеет место несанкционированное проникновение в цифровые устройства и сети и если затрагиваются персональные данные, то нарушаются также законы о защите данных. Таким образом, киберпреступность и злонамеренные манипуляции с персональными данными тесно взаимосвязаны, и применять необходимо оба свода правовых норм. Свободе в интернете угрожают обе категории киберпреступлений.

За промышленный и политический шпионаж в интернете (либо в облаке или других зонах хранения данных), то есть хищение или искажение политических фактов или коммерческих данных, кроме персональных данных, меры наказания международным правом не предусматриваются. Однако они предусмотрены

---

173 Для большинства государств – членов ЕС также имеют значение еще два международных документа: Руководящие принципы ОЭСР о защите конфиденциальности и трансграничных потоков личных данных и Европейская конвенция о защите данных Совета Европы, которая является обязательной в 46 подписавших ее государствах.

174 COM (2012)11 final.

в странах, имеющих соответствующие правовые основания согласно обычному уголовному и гражданскому праву независимо от того, является ли нарушитель частным лицом, предприятием, учреждением или иностранным правительством. В странах ЕС необходимые средства обеспечивают Будапештская конвенция и/или внутреннее законодательство. В уголовном праве это остается в силе даже в случае совершения атаки из-за национальных границ, если данное преступление привело к последствиям или причинило ущерб в пределах национальных границ. В соответствии с Конвенцией государство-член должно наказывать за киберпреступления, совершенные на его территории, и в том случае, если нарушитель не является его резидентом[175]. Таким образом, вследствие повсеместности последствий киберпреступлений уголовное право в киберсфере движется к тому, чтобы стать разделом мирового уголовного права, хотя оно еще не может быть принято всеми или применяться повсеместно, особенно в случаях, когда государство происхождения не склонно к сотрудничеству или само является нарушителем. Если слежение за данными и их перехват включают персональные данные, должны также применяться запреты и штрафные санкции, предусмотренные законами о защите данных.

Таким образом, простая истина состоит в том, что нынешнее масштабное проникновение в цифровое пространство, осуществляемое собственными или иностранными правительствами и частными структурами, согласно законодательству ЕС и сопоставимому законодательству, где оно существует, является серьезным нарушением закона, если только такое проникновение не оправдывается соображениями государственной безопасности и общественного порядка и не было санкционировано в рамках национального законодательства и требуемых правовых процедур, что придает ему законный характер. Точности ради надо отметить, что несмотря на широко распространенную практику правительств кибератаки никоим образом не могут оправдываться национальными убеждениями, субъективными требованиями безопасности и существующими правовыми процедурами того или иного иностранного правительства, пока оно не получит ясно выраженное согласие правительства страны, в которой несанкционированное проникновение осуществляется или оказывает воздействие. В ЕС совместные действия правительств государств-членов нередки и являются законными. Данные принципы охватывают широкомасштабное наблюдение за международными интернет-соединениями, узловыми пунктами, беспроводными соединениями и т. д. Еще бóльшую актуальность этому придают сообщения о масштабах неограниченного сбора данных (подлинный разгул в плане сбора) иностранными службами безопасности. Такой сбор данных основывается на использовании беспрецедентных технических возможностей и средств, но явно выходит за рамки прагматической оценки рисков и приемлемых соображений безопасности, зачастую при этом не обращается внимание на

---

175 См. пункт 233 Пояснительного доклада к Будапештской конвенции о киберпреступности.

дружественные правительства, защиту данных, права человека и причиняемый ущерб[176].

Безусловно, к этому прочтению правовой ситуации следует добавить ряд оговорок – оговорок, действие которых выходит за рамки ЕС. Во-первых, кибератаки вследствие свойственной сети анонимности трудно обнаружить. Из-за невозможности установить происхождение атаки и сложностей с обнаружением и отслеживанием во многих случаях правоохранительная деятельность становится тщетной или по меньшей мере затруднительной. В случае атаки на данные из-за границы добраться до нарушителя труднее, если государство происхождения не склонно к сотрудничеству. Это, конечно, не должно мешать нам расставить все на свои места в правовом смысле. Во-вторых, действия иностранных правительств совершаются в основном под защитой суверенитета и индивидуального дипломатического иммунитета нарушителей; однако во многих случаях деятельность по наблюдению осуществляют частные подрядчики, и тогда эта логика неприменима. Однако невозможность привлечения к ответственности – в принципе с использованием только дипломатических процедур – не изменяет основную правовую ситуацию. В странах, в которых государственный обвинитель должен действовать ex officio (в силу занимаемой должности), в случае подозрения в совершении преступных деяний, как это имеет место в большинстве стран ЕС, существует обязанность возбудить уголовное дело, если даже обвиняемый может ссылаться на суверенную неприкосновенность. В Германии в настоящее время ведется уголовное разбирательство в отношении "неустановленного лица" в целях привлечения его к ответственности за незаконное прослушивание мобильного телефона главы правительства. В интересах правовой гигиены было бы желательно, чтобы такие разбирательства проводились чаще или даже стали правилом.

В-третьих, по всей вероятности было бы разумно разработать – предпочтительно на международном уровне – доктрину цифрового наблюдения со стороны государственных служб безопасности, национальных или иностранных, без предварительного разрешения в случае "явной и непосредственной опасности", надвигающейся крупной террористической угрозы, если преступники захвачены с поличным, готовящегося серьезного преступления или нападения на ключевые объекты инфраструктуры и т. п. Разрешение всегда можно получить постфактум.

Нынешнее возмущение в большинстве европейских стран – а также в других странах – в связи с масштабным несанкционированным проникновением и шпионской деятельностью служб США представляется несколько преувеличенным и искусственно раздутым; и прежде чем пытаться найти разумные критерии, позволяющие отделить

---

176 Это убедительно показано в вышеупомянутом докладе Комиссара ООН по правам человека.

необходимое от абсолютно неприемлемого, может оказаться полезным привнести в дискуссию дух реализма и дедраматизировать ситуацию[177].

Во-первых, нельзя не учитывать беспрецедентный технический прогресс, который создает условия для масштабного несанкционированного проникновения в цифровые устройства и широкого сбора и обработки данных с использованием мощных инструментов поиска. В принципе, невозможно осуждать использование этих технологий в целях улучшения национальной политики безопасности. Эти технологии нельзя "разызобрести" обратно, и они никуда не денутся. Новым технологиям находится применение, как только они появляются, и колесо времени нельзя повернуть назад.

Во-вторых, разведывательные службы стран ЕС в равной мере пользуются этими методами часто в рамках тесного конспиративного сотрудничества со своими коллегами из США. Все они или большинство из них применяют эти технологии в своих зарубежных операциях и даже в своей стране. Это особенно относится к Соединенному Королевству, где полученные США данные и методы, разработанные в рамках программы PRISM, используются без необходимых "полномочий" или судебного контроля. Их применяют там даже в отсутствие конкретных подозрений в совершении преступления, но при этом также получают огромные объемы случайных данных в результате слежения в социальных сетях посредством подключения ко всем волоконным кабелям, проходящим через территорию Соединенного Королевства (программа TEMPORA). Таким образом, громкое возмущение во многих европейских кругах применяемыми США методами содержит элемент лицемерия.

В-третьих, достижения в сфере безопасности, обеспечиваемые методами США в борьбе с терроризмом, организованной преступностью, отмыванием денег и т. д., неоспоримы, и с учетом технологического превосходства служб США можно привести множество примеров, свидетельствующих о том, что европейские союзники входят в число основных бенефициаров.

В этом смысле можно с полным на то основанием обсуждать масштабы мер по наблюдению, но в гораздо меньшей степени – их обоснованность. Что касается масштабов, то фактически используется лишь малая доля данных, которые получены службами США или к которым они имеют доступ. По информации АНБ за 2013 год, объем данных, ежедневно циркулирующих в интернете, составляет 1828 петабайтов. АНБ может охватить только 1,2% этих данных и изучить только небольшую их часть.

---

177 Аналогичные попытки были предприняты в работах: Nigel Inkster, *The Snowden Revelations: Myths and Misapprehensions,* SURVIVAL, February-March 2014, p. 51; Joachim Krause, *Diskutieren statt moralisieren,* Internationale Politik, January-February 2014, p. 108.

Это эквивалентно всего лишь 0,0004% трафика данных в сети, и обработана фильтрами будет лишь эта часть данных[178]. Важно сохранять чувство масштаба.

И наконец, как отмечалось ранее, в США ведется здоровая дискуссия. В этой стране никогда не существовало единого мнения, а царит живая демократия, которой свойственно учиться на опыте. Имеется большая вероятность того, что протекающие в США процессы, направленные на пересмотр политики и практики в области слежения за данными и их защиты, могут в конечном счете привести к более благоприятной трансатлантической ситуации. Уже в январе 2014 года президент Обама объявил о мерах по ограничению ущерба[179]. В частности, предусматривается следующее: более строгий административный контроль за иногда ничем не ограниченными разведывательными операциями; сбор данных только строго в целях государственной безопасности; хранение данных электросвязи главным образом внутри отрасли, а доступ разведывательных служб к ним только с разрешения суда.

Приведенные выше аргументы, призванные задать тон дискуссии, никоим образом не направлены на принижение значения практикуемого в настоящее время чрезмерного и безответственного сбора данных. Нет сомнений, что существующие по разные стороны Атлантики точки зрения на слежение за данными и их защиту и на необходимые ограничения правового характера все еще далеки друг от друга во многом по историческим причинам, а также по причинам разных правовых традиций и травматического опыта, связанного с террористическими актами 2001 года. Попросту нет единого понимания соотношения между безопасностью и свободой. И едва ли это расхождение будет вскоре преодолено. Несмотря на сомнительность в правовом отношении и фундаментальное осуждение слежки и незаконного проникновения, эта практика вряд ли исчезнет даже притом, что важно понимать их ассоциацию с преступной деятельностью и наказуемость по закону. "Слежка за союзниками" – особенно болезненный вопрос, затрагивающий товарищеские отношения, единство цели и даже узы личной дружбы, однако у нее давние традиции даже в трансатлантическом контексте. Однако если не считать того, что речь идет о нарушении этикета – доверия, мало шансов на то, что союзники бросятся заключать

---

178 Данные из работы Joachim Krause, ibid p. 114. С учетом того, что их источником является АНБ, некоторые сомневаются в достоверности этих цифр, однако они, даже будучи ориентировочными данными, показывают, что Агентство не может следить более чем за небольшой долей трафика в интернете, что оно сосредоточивает усилия на частичных данных, относящихся к безопасности, и что оно по-прежнему захватывает далеко не все данные.

179 Президентская политическая директива PPD 28, www.whitehouse.gov.

официальные соглашения об отказе от слежки[180]. Приветствовались бы неофициальные договоренности.

Много чернил потрачено, чтобы предложить решения, направленные на преодоление трудностей, связанных с наблюдением, особенно в отношениях между ЕС и США. В настоящее время ведутся общественные дискуссии и обсуждения между правительствами, и поэтому было бы самонадеянно произносить проповедь с твердыми и исчерпывающими рекомендациями для всех участников. Вместо этого в конце данной статьи будет приведен лишь весьма скромный совет.

Что касается ЕС, важно в ближайшее время окончательно оформить правовые документы, призванные завершить создание связанных с кибербезопасностью компонентов Цифровой повестки дня ЕС – Директиву по сетевой и информационной безопасности (NIS) и Генеральный регламент по защите данных (GDPR) – в качестве единой основы для любых будущих соглашений с США и другими странами мира.

Государства – члены ЕС должны также позаботиться о том, чтобы их собственные разведывательные службы строго соблюдали европейское и национальное законодательство. Не имело бы смысла просить от США большего, чем делает ЕС. Странам ЕС следует также заключить между собой соглашение о взаимном отказе от слежки в рамках всего ЕС и рассмотреть возможность постепенного создания разведывательной службы ЕС с обменом полной информацией между странами Союза. Тем временем следует еще более улучшить координацию действий между их службами безопасности.

Необходимо активизировать применение в ЕС законов по вопросам киберсферы и защиты данных, чтобы показать, что предусматривается законом применительно к теневым разведывательным операциям и шпионажу.

Как показано в одной из предыдущих глав, лучшая киберзащита основывается на повышенной способности к восстановлению в киберсреде, что также относится к противодействию незаконному сбору данных и информационным атакам. Есть много возможностей для укрепления технической способности систем и сетей к восстановлению, усиления самозащиты пользователей (повышение осведомленности по вопросам безопасности, улучшение информационной экономики и методов резервного копирования, шифрование и т. д.). Иными словами, прежде чем жаловаться, займитесь тем, что зависит от вас.

Восстановление кибердоверия в трансатлантическом контексте – трудная задача, которая может принести плоды лишь со временем. Однако наступила пора заняться выработкой транспарентного совместного понимания того, как можно найти прочный

---

180 См.: Leif-Eric Easley, *Spying on Allies.* SURVIVAL, August-September 2014, p. 141; Rodri Jeffreys Jones, *Eine Frage der Etikette,* Internationale Politik, September-Oktober 2014, p. 74.

баланс между свободой и требованиями безопасности и как можно обеспечить совместимость разведывательной работы и наблюдения со стороны иностранных государств с положениями внутреннего законодательства ЕС. Неоспоримо, что иностранные агенты должны придерживаться норм страны, в которой они работают. В этой связи трансатлантические расхождения, возможно, не удастся преодолеть в ближайшее время, но их следует уменьшить. ЕС явно не может отойти от своих высоких стандартов защиты данных. Следует начать работу по пересмотру Соглашения о "безопасной гавани", регулирующего такие вопросы, как обязательные требования к трансграничной передаче данных и их безупречное исполнение.

После нынешнего всплеска несанкционированного доступа к данным, чрезмерный характер которого широко признается, должна сформироваться новая атмосфера, характеризующаяся соразмерностью и сдержанностью, в которой колоссальные технические возможности сбора данных используются умеренно, с учетом интересов затрагиваемых лиц, включая права человека, и с соблюдением правовых норм стран, в которых осуществляется поиск. Нам нужна культура более трезвой оценки потребностей безопасности и сдержанности.

В среднесрочной перспективе должна восторжествовать глобальная точка зрения. ЕС должен принять участие в усилиях по созданию международной нормативной базы в полном соответствии с резолюцией A/RES/68/167 Генеральной Ассамблеи, содействуя тем самым достижению устойчивого баланса между общими интересами безопасности и свободой в интернете.

3.5 Пределы киберсвободы: в поисках критериев

Вильям А. Барлетта

Технологии цифровой электросвязи, примером которых является в первую очередь интернет, оказывают носящее подрывной характер воздействие на общество, сравнимое по масштабам только с электрификацией больших и малых городов более века назад. Как и электрификация, цифровая электросвязь зависит от наличия широко распространенных взаимосвязанных сетей. Однако в отличие от сетей энергоснабжения (энергетических систем), которые являются региональными по масштабу, интернет охватывает весь мир, пересекая национальные границы и преодолевая культурные барьеры. Подобно тому как не охваченными программами электрификации остаются примерно два миллиарда "энергетических бедняков", интернет недоступен относительно большому классу "информационных бедняков". Как и в случае современных энергетических систем, которые позволяют потребителям передавать и получать энергию, пользователи интернета регулярно как передают, так и получают информацию, часто в равной мере.

Таким образом, подобно анализу энергетических сетей с правовой и политической точек зрения, анализ средств обеспечения информационного общества породил собственные термины справедливого распределения и морального долга. Свобода[181] является именно таким термином – термином, который побуждает многих рассматривать свободу в интернете как одно из основных прав человека, определенных в принятой ООН Всеобщей декларации прав человека[182] (ВДПЧ*).* В частности, статья 19 ВДПЧ гарантирует право на свободу выражения мнений.

Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ.

В своем докладе Уэстби[183] отмечает: "Хотя ВДПЧ не является непосредственно обязательной для государств – членов ООН, некоторые ее части, в том числе статья 19, приобрели юридическую силу в качестве обычного международного права. Формулировка статьи 19 "беспрепятственно […] искать, получать и распространять информацию и идеи […] независимо от государственных границ" хорошо согласуется с обычным описанием свободы в интернете, которое включает свободу доступа. Некоторые могут трактовать слово "беспрепятственно" как предполагающее право на неприкосновенность частной жизни, анонимность, защиту данных и даже право удалять контент, размещенный ими в сети".

Согласно статье 19 *доступ* к интернету можно рассматривать в качестве одного из критериев для оценки свободы в интернете. Статья 19 также подразумевает, что другими критериями оценки свободы в интернете являются ограничения контента (или *использования*) и степень вмешательства (неприкосновенность частной жизни и целостность контента). Международная правозащитная организация Freedom House проводит ежегодную оценку[184] состояния свободы в интернете. В своем докладе за

---

181 Свободу в интернете называют гибким термином, который используется США и их европейскими союзниками в борьбе за будущую власть над интернетом. См.: "World War 3.0," Vanity Fair, May 2012.

182 Резолюция 217A (III) Генеральной Ассамблеи ООН, 10 декабря 1948 года, http://www.un.org/en/documents/udhr/.

183 J.R. Westby, The Role of Science and Technology as Empowerment of Person and State, Proceedings of 44th Session, International Seminars on Planetary Emergencies, 19-24 August 2011, Erice, Sicily.

184 Организация Freedom House применяет трехкомпонентный подход к определению уровня свободы в интернете и в области ИКТ:

- препятствия на пути доступа – включая инфраструктурные и экономические барьеры на пути доступа, юридический контроль за поставщиками услуг интернета (ПУИ) и контроль в силу прав собственности и независимость регуляторных органов;

2013 год[185] она делает вывод о том, что с середины 2012 года в 34 подвергшихся оценке странах из 60 "наблюдается негативная динамика, а в 16 странах – позитивная динамика".

Такие показатели можно назвать характеристиками свободы от репрессий, особенно когда интернет используется для выражения социального недовольства, организации оппозиционных политических сил или просто распространения информации, которая может быть неприятной для лиц, занимающих влиятельные позиции в обществе. Члены этой группы много писали на тему расширения прав и возможностей граждан с помощью интернета и киберрепрессий в отношении них[186]. Уэстби четко изложил эту проблему: "*Интересы национального государства противоречат правам индивида, при этом ИКТ являются наилучшим инструментом для укрепления власти с обеих сторон*"[187].

То, что в "свободных" обществах сводится к реально трудной проблеме определение критериев постоянного политического баланса между свободой и вмешательством государства в четких правовых рамках, во многих других государствах становится проблемой прав человека и качества глобального информационного порядка. Правительственная цензура интернета посредством технологий фильтрации без законодательных ограничений и с серьезными и острыми последствиям для людей,

---

- ограничения контента – включая правовые нормы в отношении контента, техническую фильтрацию и блокирование веб-сайтов, самоцензуру, активность/разнообразие онлайновых средств массовой информации и использование ИКТ для гражданской мобилизации;
- нарушения прав пользователей – включая слежение, неприкосновенность частной жизни и последствия онлайновой деятельности, такие как тюремное заключение, внеправовые притеснения или кибератаки.

Доклады этой организации размещены по адресу http://www.freedomhouse.org/reporttypes/freedom-net#.VBB2dUhA140.

185 Freedom on the Net 2013, A Summary of Findings, p. 2. Размещено по адресу http://www.freedomhouse.org/report/freedom-net/freedom-net-2013#.VBB6CUhA140.

186 H. Wegener, “Cyber Repression: Going Worse. What can be done?,” Proceedings of the International Seminars on Planetary Emergencies, Erice, (2011), "Последствия всеобъемлющей цензуры – киберрепрессии – являются серьезными, и их невозможно переоценить. Граждане отсекаются от важных преимуществ информационного века и получают искаженное представление о реальном положении в мире, что обрекает их на политическую незрелость. Широкомасштабные киберрепрессии могут изменить коллективные умонастроения в стране. По степени опасности широкомасштабное замалчивание информации сопоставимо с другими видами киберпреступлений и киберконфликтов …"

187 Westby, op. cit.

собирающих и передающих информацию, является значительным нарушением прав человека[188].

В то время как эти трения легче всего устранить путем изменения поведения государств, отсутствие централизованного управления использованием интернета в сочетании с его сильно рассредоточенной структурой позволяет неправительственным организациям и корпоративным структурам значительно ограничивать свободу в интернете для целевых групп. Интернет настолько усилил влияние негосударственных субъектов, что правительства находят привлекательным принуждать корпорации[189] выполнять цензорские функции, осуществлять контроль за использованием и т. д.

В странах, имеющих производящие интернет-технологии отрасли, можно было бы рассмотреть возможный подход к выравниванию степени свободы доступа в глобальном масштабе. Правительства таких стран могли бы запретить экспорт или по меньшей мере потребовать представления отчетности об экспорте "товаров и технологий, которые могут способствовать получению каким-либо зарубежным правительством возможности осуществлять цензуру, наблюдение или любую другую соответствующую деятельность с использованием средств электросвязи, включая интернет"[190]. Хотя действенность таких мер является спорной, они привлекают внимание к взаимодополняющему характеру действий государств и отраслей в вопросе установления пределов свободы в интернете.

Как большинство запаздывающих индикаторов поведения, эти негативные показатели представляют не всю картину. Столь же показательны, хотя и вызывают больше трудностей с точки зрения количественной оценки, действия, повышающие социальное и экономическое благополучие общества. Жесткое управление с четко сформулированной целью обеспечения стабильности, безопасности и способности сети к восстановлению может привести к сдерживанию изобретательского творчества, подавлению новых сетевых парадигм и технологической открытости.

Неудивительно, что законные (коллективные) интересы национальных государств могут вступать в противоречие с интересами отдельных лиц в киберпространстве. Эти интересы включают, в частности, защиту граждан от общепризнанных негативных

---

188 Вегенер, МСЭ, 2011 год, с. 46.

189 "В 2008 году правительство США угрожало компании Yahoo штрафом в размере 250 тыс. долл. США в сутки, если она не выполнит общий запрос о предоставлении данных пользователей, который компания считала неконституционным, как явствует из судебных документов, рассекреченных в четверг". *U.S. threatened massive fine to force Yahoo to release data*, Washington Post, 11 September 2014.

190 Палата представителей США, H.R.3605 – Акт о глобальной свободе в сети, 2011 год.

воздействий, например сохранение социальных (культурных) норм, предупреждение чудовищных преступлений[191] и терроризма, предотвращение перебоев в работе ключевых объектов социальной инфраструктуры (включая интернет и другие объекты IT-инфраструктуры), защиту законных государственных тайн, содействие проведению внешней политики государства и содействие обеспечению национального экономического благополучия, особенно путем воздействия на внешние факторы. Хотя за пределами киберсферы правила игры при продвижении конкурирующих интересов государств хорошо отработаны, в киберпространстве возникают создающие помехи трудности вследствие 1) отсутствия согласованной правовой базы, регулирующей поведение в киберпространстве, и 2) значительных исторически обусловленных культурных различий, которые часто встречаются в глобальной сети, пересекающей множество национальных границ.

Можно привести показательный пример. В странах ЕС, как правило, существуют жесткие запреты в отношении контента, который они определяют термином "язык вражды" или его соответствующим эквивалентом[192]. Эти запреты связаны с гибелью большого числа людей во время Второй мировой войны. В некоторых мусульманских государствах также имеются аналогичные жесткие запреты на распространение других религий[193] или распространение кощунственных слов о пророке Мухаммеде или его изображений. В обоих случаях запреты отражают строгие культурные нормы, нарушение которых может привести к социальной розни и даже насилию. Когда правительства блокируют такие сайты, совершают ли они носящее репрессивный характер нарушение прав человека?

Напротив, в США расширительно толкуют понятие допустимого высказывания, которое закреплено в их конституции. Видный американский ученый-правовед Лоренс Трайб[194] (с коллегой) пишет:

> "Слово обладает большой силой. Оно – источник жизненной силы демократии, непременное условие установления истины и крайне

---

191 Одним из общепризнанных примеров является международное сотрудничество полицейских органов в целях искоренения детской порнографии.

192 Например, французский суд обязал компанию Yahoo удалить со своего аукционного сайта нацистскую атрибутику. Разве это хуже принуждения Китаем компании Yahoo к подписанию "добровольного обязательства" об отказе от "производства, размещения и распространения вредной информации, которая может угрожать безопасности государства и нарушать социальную стабильность"? Christopher Bodeen, "Web Portals Sign China Content Pact," Associated Press, 15 July 2002.

193 Hillary Clinton, "Internet Freedom", http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom.

194 Lawrence Tribe and Joshua Matz, Uncertain Justice, (New York, 2014) p. 123.

> необходимо для нашего саморазвития. Однако слово также опасно. Оно может разрушать демократию, создавать условия для преступления или подстрекать к его совершению, поощрять врагов и мешать управлению государством. Его можно использовать как оружие и обращать против неуступчивых объектов воздействия".

Однако даже в США ограничения свободы слова в целях пресечения проявлений "языка вражды" и "кибербуллинга" получают более широкое распространение. В американском обществе, в высокой степени склонном отстаивать свои права в суде, ограничения все еще не принимают вид предварительных запретов на высказывания, а являются основанием для деликтного иска или даже уголовных наказаний.

Помимо физического блокирования доступа к сайтам, правительства могут сделать стоимость доступа неприемлемо высокой, чтобы по сути серьезно ограничить доступ по политическим соображениям. Например, наблюдение за сайтами с "опасным" и/или провокационным либо незаконным контентом в целях отслеживания и ограничения доступа тех, кто их посещает, может сопровождаться применением тайных процедур, направленных против свободы лиц, посещающих эти сайты. Из-за ошибок при слежении за "террористическими" сайтами многие люди оказались включенными в черные списки пассажиров авиакомпаний. Хотя легко признать наличие насущной заинтересованности государства в таких программах наблюдения, вызывает тревогу отсутствие открытых судебных процедур, обеспечивающих учет интересов отдельных лиц.

Между странами наблюдаются значительные расхождения в политике в области анонимности и неприкосновенности частной жизни. Многие воспринимают анонимность при общении в интернете как право. Поскольку анонимность может защитить автора высказывания от преследования или мести, она воспринимается как жизненно важное условие свободы слова. Более того, США признают[195] право на анонимное ведение политических кампаний; они также подтвердили право на анонимное взаимодействие между людьми "при условии, что эти действия не нарушают закон"[196]. Тем не менее США не приняли общей политики в отношении анонимности и неприкосновенности частной жизни в интернете, предпочитая регулировать конкретные отрасли. Занимая более решительную позицию, ЕС предпочитает непосредственно регулировать вопросы права лиц на неприкосновенность частной жизни и анонимность.

---

195 US Supreme Court, McIntyre v. Ohio Elections Commission (93-986), 514 U.S. 334 (1995).

196 Decision *Columbia Insurance Company v. Seescandy.com, et al.* of the U.S. District Court in the Northern District of California.

В то же время анонимность может служить удобным прикрытием для деструктивных и преступных действий. В числе стран, вводящих другие ограничения, которые ужесточают контроль за использованием интернета, Россия в настоящее время установила запрет на анонимный доступ к сетям Wi-Fi в общественных местах[197], где IP-адрес не может быть однозначно увязан с конкретными лицами. Кроме того, как показали разоблачения Сноудена, правительство США настаивает на крайне широком (и, возможно, безграничном) праве следить за общением в интернете. И следят за использованием интернета не одни только правительства – за его использованием также широко следят такие крупные корпорации, как Google. Неудивительно, что различные пользователи теперь получают в интернете индивидуально настроенные (или адресные) услуги, хотят они этого или нет.

Широкое использование США средств массового слежения и прослушивание средств связи глав дружественных правительств, как показали разоблачения Сноудена, позволяют предположить, что при использовании средств электросвязи действительная конфиденциальность обеспечивается крайне редко или вовсе не обеспечивается. К сожалению, полноценное общественное обсуждение масштабов, мотивов и видов такой деятельности государства, как правило, выведено даже из-под судебного контроля со ссылкой на привилегию государственной тайны[198]. Приводимое правительством США в качестве оправдания утверждение "это делают все" вряд ли может успокоить. На самом деле в условиях резкого роста возможностей компьютеров и объемов памяти на единицу затрат практически любое промышленно развитое государство может осуществлять контроль за всем трафиком в интернете, входящим в страну или исходящим из нее. В наиболее экономически развитых странах возможен сплошной контроль за всем трафиком при соучастии (вынужденном или добровольном) поставщиков услуг электросвязи.

Характер реакции общественности как в США, так и в Европе на сообщения о почти повсеместном слежении за трафиком сотовой телефонной связи побудил компанию Apple выпустить свою новейшую операционную систему для сотовых телефонов (iOS8) с мощной криптографической защитой без возможности ее обхода. Поэтому даже компания Apple не может снять криптографическую защиту телефона по судебному

---

197 Медведев подписал постановление, запрещающее анонимный Wi-Fi, http://en.itar-tass.com/russia/744055, *8 августа 2014 года.*

198 Привилегия государственной тайны является доказательственным правилом, сложившимся на основании судебного прецедента в Соединенных Штатах. Ссылка на эту привилегию приводит к исключению доказательств […] исключительно на основании представленных правительством письменных показаний, в которых говорится, что при судебном разбирательстве может быть разглашена конфиденциальная информация, которая может угрожать национальной безопасности. Первым делом, в котором эта привилегия получила официальное признание, было связанное с военной тайной дело "Соединенные Штаты Америки против Рейнольдса", http://en.wikipedia.org/wiki/State_secrets_privilege.

приказу[199]. В то время как критики компании Apple настойчиво утверждают, что iOS8 "лишь препятствует законным расследованиям, проводимым на законных основаниях"[200], ее защитники считают, что Apple "создает системы, которые не позволяют получить доступ к вашему телефону всем, кому могут понадобиться ваши данные, включая хакеров, внутренних злоумышленников и даже враждебные иностранные государства. Это полностью отвечает общественным интересам. Кроме того, компания Apple при этом создает прецедент: ключи от собственных устройств должны находиться у пользователей, а *не* у компаний"[201]. Официальная ведомственная реакция правительства США пока не известна; однако ряд государственных должностных лиц осудили[202] подход компании Apple. Не вызвала бы удивления официальная ведомственная реакция, носящая характер скорее принуждения, чем морального убеждения.

Ранее США пытались установить для производителей аппаратных средств требования, обеспечивающие возможность слежения, установления личности и расшифровки трафика в интернете. При описании того, как Государственный департамент США работает "над защитой и поддержкой свободного и открытого интернета" в качестве элемента своей политики[203], госсекретарь Клинтон пояснила[204]:

> "Все общества признают, что у свободы слова есть свои пределы. Мы не миримся с теми, кто подстрекает других к насилию, например с агентами

---

199 Кодекс конфиденциальности компании Apple: "Наше приверженность защите конфиденциальности клиента не исчезает из-за запроса информации правительством", https://www.apple.com/privacy/government-information-requests/. См. также: Matthew Green, "Is Apple picking a fight with the US government," Slate 23 September 2014. Размещено по адресу http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html.

200 Oren Kerr, "Apple's dangerous game," http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/Kerr. Автор несколько изменил свои взгляды, признав, что система с возможностью обхода криптографической защиты может быть взломана любым желающим и поэтому ставит под угрозу безопасность всей системы в целом.

201 Matthew Green, Ibid.

202 В интервью новой программе CBS "60 минут" 12 октября 2014 года директор ФБР Джеймс Карни обвинил компанию Apple в том, что ее новая функция обеспечения конфиденциальности защищает похитителей людей, педофилов и террористов. См.: http://money.cnn.com/2014/10/13/technology/security/fbi-apple/index.html?hpt=hp_t2.

203 US State Department, "International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World," http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

204 Clinton, op. cit.

> "Аль-Каиды", которые – в данный момент – используют интернет для поощрения массового убийства невинных людей. Мы осуждаем также целенаправленное использование "языка вражды" в отношении отдельных лиц по признаку их этнической принадлежности, пола или сексуальной ориентации. К сожалению, обе эти проблемы порождают все бóльшие трудности, с которыми международное сообщество должно справляться совместно. Мы должны также попытаться решить проблему анонимности высказываний. Те, кто использует интернет для вербовки террористов или распространения краденой интеллектуальной собственности, не могут отделить свою деятельность в интернете от своей личности в реальном мире".

Одновременно при этом ФБР предупредило владельцев интернет-кафе в США, "что использование определенных простейших мер кибербезопасности может быть сочтено основанием для подозрений в возможной террористической деятельности"[205].

Аналогичные противоречия между интересами отдельного лица и государства существуют также в развивающихся странах, при этом в промышленно развитых странах криптография считается оружием, в равной мере доступным как законопослушным гражданам, так и преступникам и террористам.

В Африке законы, относящиеся конкретно к шифрованию, существуют, как представляется, только в государствах Северной Африки – Алжире, Египте, Марокко и Тунисе, а также в Нигерии и Южной Африке. В Африке одной из первых закон о криптографии приняла Южная Африка, однако этичность [южноафриканского] закона о раскрытии ключа оспаривается некоторыми энтузиастами по соображениям соблюдения прав человека. Для некоторых криптография представляется единственным решением проблемы угроз конфиденциальности, по мере того как человеческое общество адаптируется к переходу мировых сетей на цифровые технологии[206].

В настоящее время мощная криптографическая защита с симметричным ключом, например по стандарту OpenPGP, запросто доступна любому человеку, который не проживает в государстве, поддерживающем терроризм, согласно определению Государственного департамента США. Трудно представить себе, что это ограничение может долгое время сдерживать реальные террористические ячейки. Так же трудно

---

205 Vanity Fair, op. cit.

206 Cory Farmer and Judson L. Jeffries, “Telecommunications Surveillance and Cryptography Regulatory Policy in Africa,” African Policy Journal, May 2013. Размещено по адресу http://apj.fas.harvard.edu/category/articles/.

представить себе, что сторонники шифрования военного уровня будут рады предложениям с требованием передачи "ключей добровольного депонирования" судебным органам своего правительства[207].

Возможность для конфликта между правительствами, защищающими то, что они считают законными интересами своих граждан, очевидна. Однако именно в тех случаях, когда в ходе совершения предполагаемых правонарушений пересекается множество национальных границ, пострадавшее государство мало что может сделать для исправления положения, кроме как заблокировать адрес протокола Интернет (IP-адрес), с которого совершено правонарушение. Одним из серьезных препятствий является отсутствие согласованной правовой базы, регулирующей поведение в киберпространстве. Даже в тех случаях, когда деяние, совершенное в киберпространстве, считается тяжким преступлением в государстве предполагаемой жертвы, предполагаемый преступник может находиться вне досягаемости закона[208].

В тех случаях, когда эти интересы граждан формулируются исходя из прав человека, а не обеспечения баланса конкурирующих законных интересов, ставки как для отдельных лиц, так и для общества повышаются. Винт Серф[209], инженер и пионер интернета, отметил:

---

207 В этом сценарии секретные ключи хранились бы под многоуровневой защитой в неактивном состоянии с возможностью доступа только при наличии надлежащих оснований и инструкций по дешифровке. Cory and Farmer, Ibid, p. 3.

208 Для того чтобы страна могла проводить расследования и привлекать виновных к ответственности, сотрудники ее правоохранительных органов должны иметь возможность собирать информацию и доказательства в других странах. Основным препятствием на пути расследования, в случае если доказательства и подозреваемые находятся по разные стороны национальных границ, является необходимость соблюдения сотрудниками правоохранительных органов суверенитета других стран. Сотрудники правоохранительных органов одной страны, как правило, не могут въезжать в другую страну, чтобы расследовать версии, собирать доказательства и задерживать подозреваемых. Соответственно, для международных расследований требуются сотрудничество и помощь властей стран, в которых находятся жертвы, доказательства и подозреваемые. Даже если подозреваемые установлены, страны обычно не допускают выдачи своих граждан, утверждая при этом, что привлечение к ответственности должно осуществляться в самой стране, зачастую на том основании, что выдача противоречит их юрисдикционной базе, приведет к нарушению средств индивидуальной защиты, гарантированных их гражданам, и к более значительным препятствиям, связанным с доказательствами, при судебном разбирательстве. Однако обвинители пришли к заключению, что страны, которые не соглашаются выдавать своих граждан, не обеспечивают на систематической основе привлечение к ответственности в своих пределах. G. A. Barletta, частное сообщение, 201.

209 Один из общепризнанных "отцов интернета".

"Технология является инструментом реализации прав, но не собственно правом. Чтобы что-то рассматривалось в качестве права человека, оно должно удовлетворять высоким критериям. Грубо говоря, оно должно входить в набор необходимого нам как человеческим существам, чтобы вести здоровую, содержательную жизнь, как, например, свобода от пыток или свобода совести. Включать любую конкретную технологию в эту высокую категорию – ошибка, потому что со временем окажется, что мы ценим не то, что следует"[210].

К сожалению, предоставление свободы в интернете (свободы доступа) как права человека дает возможность в рамках политической дискуссии ставить идеологию выше здравого смысла. Независимо от того, идет ли речь о "сетевом нейтралитете" или "открытом доступе" к публикациям, как полоса пропускания, так и обработка контента стоят денег. Слишком часто идеологи стремятся гарантировать "нейтралитет" и "доступ" как необеспеченное обязательство, исходя из того, что "кто-то другой – обычно издатель – заплатит", при этом зачастую аргумент[211] формулируется в контексте гарантии свободы в интернете. Тем не менее широкий доступ и минимизация инфраструктурных барьеров являются желанными целями, которые могут быть достигнуты при использовании многих возможных бизнес-моделей.

Отрасль играет одну из главных ролей как в создании цифрового общества, так и в управлении им. Нынешняя свобода действий в интернете в большой степени является заслугой частного сектора. Испытывая давление со стороны правительств, требующих от них содействия репрессивным мерам, корпорации в то же время создают широкие альянсы с правозащитными группами, учеными, инвесторами и организациями гражданского общества, чтобы противостоять такому давлению. Достойной внимания мерой является Глобальная сетевая инициатива[212] (GNI). В рамках GNI было представлено ви́дение[213] роли определяющих факторов угроз "свободе выражения мнений и неприкосновенности частной жизни" в отрасли. Отмечается, что быстрыми темпами идет внедрение новых технологий (как аппаратных средств, так и программного обеспечения) и новых продуктов обеспечения безопасности. Эти продукты несут с собой новые риски и новые возможности с точки зрения свободы в интернете. Хотя у отрасли практически нет возможностей непосредственно контролировать действия конечных пользователей технологий, она может дать наиболее квалифицированные в техническом отношении рекомендации поставщикам

---

210 V. Cerf, “Internet Access is Not a Human Right”, New York Times, 4 January 2012.

211 Примером служит материал в разделе "Мнения". "A Threat to Internet Freedom," B. Knappenburger, New York Times, 9 July 2014.

212 https://globalnetworkinitiative.org/

213 D.A. Hope, "Protecting Human Rights in the Digital Age," February 2011, http://www.globalnetworkinitiative.org/cms/uploads/1/BSR_ICT_Human_Rights_Report.pdf.

услуг электросвязи, направленные на минимизацию зарождающихся угроз свободе в интернете.

В последние несколько лет отрасль ИКТ все более активно определяет подходы к защите свободы выражения мнений и неприкосновенности частной жизни. Например, Глобальная сетевая инициатива предоставляет компаниям инструкции и рекомендации о том, как реагировать на требования правительства об удалении, фильтрации или блокировании контента и как реагировать на требования правоохранительных органов о раскрытии персональной информации. Эти виды определяющих факторов угроз будут иметь значение для компаний, которые хранят большие объемы персональной информации и/или выступают в роли "стражей" контента, главным образом поставщиков услуг электросвязи и компаний, предоставляющих услуги интернета.

Можно ожидать, что по мере развития аппаратных средств и появления оборудования с мощной защитой, встроенной на уровне интегральной схемы, правительства будут оказывать на производителей еще более сильное давление, требуя оставить возможность обхода защиты для правительств (правоохранительных и разведывательных органов) в целях наблюдения, слежения за отдельными лицами, отслеживания действий в интернете и получения доказательств для судебных разбирательств. Что выглядит еще более зловеще, могут быть разработаны продукты с такими свойствами, которые позволят осуществлять цензуру и устанавливать ограничения для контента на уровне микросхемы. Хотя отрасль находится в фокусе давления, оказываемого в целях ограничения свободы, она также обладает наибольшей квалификацией и находится в наиболее выгодном положении, чтобы противостоять такому давлению.

Быстрое реагирование отрасли на множащиеся угрозы безопасности ИКТ и информации, которая создается, передается, принимается и хранится с их помощью, является одной из важнейших гарантий свободы использовать цифровую информацию по своему усмотрению как для частных лиц, так и для учреждений. Такая свобода предполагает уверенность конечного пользователя в принадлежности

информации[214], правах пользователя[215], достоверности[216] и конфиденциальности данных[217]. Некоторые могут включить в этот список возможность удаления данных из интернета и правовые гарантии принуждения к раскрытию паролей к личным сайтам не иначе как по судебному приказу. Угрозы свободе использования исходят от широкого круга субъектов – от отдельных хакеров до преступных групп и финансируемых государством групп.

Личную свободу в способной к восстановлению и защищенной инфраструктуре интернета нельзя обеспечить по чистой случайности. Должны быть предприняты позитивные действия, направленные на то, чтобы сбалансировать интересы государства, с одной стороны, и отдельных лиц и частного сектора – с другой, при одновременном обеспечении защиты всех пользователей от злонамеренных субъектов. Можно ожидать, что в разных обществах характер действий государства будет разным.

Что касается западных стран, мы хотели бы рассчитывать на то, что в них будет использоваться в основном судебный контроль – будь то в конфиденциальном порядке[218] или нет – для вынесения решений по отдельным делам вместо выдачи массовых разрешений правоохранительным и разведывательным органам. Активное участие отрасли – как производителей аппаратных средств, так и разработчиков программного обеспечения – могло бы обеспечить рост уровня безопасности и

---

214 [Предполагаемые] владельцы информации часто требуют юридической защиты прав на ее распространение и использование. Владелец может установить критерии использования информации, или даже контроль за доступом к информации. Такие критерии могут включать права на дальнейшее распространение информации уполномоченным пользователем (или организацией-пользователем). Такой контроль применяется в целях обеспечения безопасности государственной информации, защищенной исключительными правами информации, и персональной конфиденциальной информации. Лицемерные [и легалистические] нападки на права собственности могут понизить полезность информации даже до такой степени, что она останется без исковой защиты.

215 Владелец информации может установить критерии использования информации или даже контроль за доступом к ней. Такой контроль типичен в тех случаях, когда информация считается защищаемой законом об интеллектуальной собственности.

216 Пользователь данных должен (и может быть обязан по закону) оценивать (и, возможно, документировать) свой уровень доверия к создателю данных и источнику (поставщику), а также фактические неточности в содержании данных (таких, как данные измерений, данные учета транзакций, статистические данные и т. д.). Нападки на достоверность информации направлены на снижение полезности данных и подрыв доверия заинтересованных сторон к компетентности сторон (и учреждений), использующих эти данные.

217 Особенно важно для частных лиц в случае конкретной персональной информации.

218 Например, суды по контролю за внешней разведкой США (FISA). Одних лишь административных комиссий недостаточно.

конфиденциальности для пользователей. Действуя совместно, поставщики услуг интернета могли бы управлять на конфиденциальной основе долгосрочным сбором и хранением данных пользователей, которые будут доступны правительству только на четких и транспарентных условиях. Должно быть установлено некое правило соразмерности, беспредельному несанкционированному проникновению правительств в сети и сбору ими данных должен быть положен конец, должно осуществляться международное сотрудничество по вопросу определения условий слежки за союзниками и должны быть разработаны соглашения, подобные Соглашению о "безопасной гавани"[219]. Фактическая правовая база должна стать результатом законодательной деятельности, основанной на полномасштабной, открытой общественной дискуссии и консультациях с союзниками и международными органами.

В то же время Китай создал собственный национальный интернет:

> "Китайский авторитарный режим не только выжил в условиях существования интернета, но и благодаря проявленному государством большому искусству в использовании этой технологии в собственных целях, позволившему ему укрепить контроль за собственным обществом, показал пример другим репрессивным режимам. Китайское однопартийное государство развернуло целую армию киберполиции, инженеров по аппаратуре, разработчиков программного обеспечения, специалистов по мониторингу интернета и платных онлайновых пропагандистов, которые осуществляют контроль, фильтрацию, цензуру и руководство китайскими пользователями интернета. Китайским частным интернет-компаниям, многие из которых являются клонами западных компаний, разрешается успешно развиваться при условии, что они не отклоняются от линии партии.
>
> [...] Китайский интернет напоминает огороженную игровую площадку с патерналистской охраной. Как и интернет, которым пользуются в большей части остального мира, он беспорядочен и недисциплинирован, он предлагает разнообразные услуги, такие как игры, совершение покупок и многое другое. Предоставление собственному китайскому интернету возможности процветать было важным элементом создания усовершенствованной клетки. Однако за ним постоянно следят и манипулируют им"[220].

По мере продажи своих технологий за рубежом – в странах Центральной и Юго-Восточной Азии, Восточной Европы и Африки – Китай обретает союзников в своем споре с США и ЕС по поводу управлением использованием интернета.

---

219 https://safeharbor.export.gov/list.aspx

220 "China's Internet: A giant cage", The Economist, 6 April 2013.

Результаты этого спора, вероятно, определят границы в интернете в глобальном масштабе.

Список сокращений

APS	Американское физическое общество
ARPANET	Сеть связи Управления перспективных научно-исследовательских проектов
CAPTEL	Центр права и политики в области технологий Азиатско-Тихоокеанского региона
CBM	Меры по укреплению доверия
CCDCOE	Центр передового опыта по совместной защите от киберугроз
CERT	Группа реагирования на нарушения компьютерной защиты
CIRT	Группа реагирования на компьютерные инциденты
COP	Инициатива "Защита ребенка в онлайновой среде" (МСЭ)
EC3	Европейский центр по борьбе с киберпреступностью (Европол)
EEAS	Европейская служба внешнеполитической деятельности (Европейский союз)
ENISA	Европейское агентство по сетевой и информационной безопасности
EPFL	Федеральная политехническая школа Лозанны
G8	Группа восьми
GDPR	Генеральный регламент по защите данных
GNI	Глобальная сетевая инициатива
GPS	Глобальная система определения местоположения
HLEG	Группа экспертов высокого уровня
HRC	Комитет по правам человека (КПЧ)
ICANN	Корпорация Интернета по присваиванию наименований и номеров
ICSC	Международный центр научной культуры
INDECT	Интеллектуальная информационная система, поддерживающая наблюдение, поиск и обнаружение для обеспечения безопасности граждан в городской среде

IP	Протокол Интернет
ISF	Форум по информационной безопасности
ITIS	Институт интеллектуальных систем
LINC	Ливанский центр по вопросам интернета
LITA	Ливанская ассоциация информационных технологий
MAC	Обязательное управление доступом
MIT	Массачусетский технологический институт
NIS	Сетевая и информационная безопасность
PDA	Персональный цифровой помощник
PGP	Компьютерная программа шифрования данных с высокой степенью надежности (программа Pretty Good Privacy)
PMP	Постоянная группа по мониторингу информационной безопасности (WFS)
RFID	Радиочастотная идентификация
SaaS	Программное обеспечение как услуга
SAFECode	Форум по обеспечению высокого качества кода программного обеспечения
SCADA	Диспетчерский контроль и сбор данных
SIL	Уровень полноты безопасности
SLA	Правовой договор на обслуживание
SMAC	Социальные, мобильные, аналитические и облачные технологии (технологии SMAC)
SOA	Сервис-ориентированная архитектура
TCP	Протокол управления передачей
UCLA	Лос-анджелесский университет Калифорнии
UDHR	Всеобщая декларация прав человека (ВДПЧ)
US-CERT	Группа реагирования на нарушения компьютерной защиты США
WFS	Всемирная федерация ученых

АНБ	Агентство национальной безопасности
АСЕАН	Ассоциация государств Юго-Восточной Азии
АФАКТ	Азиатско-Тихоокеанский совет по упрощению процедур торговли и электронным деловым операциям
ВВУИО	Всемирная встреча на высшем уровне по вопросам информационного общества
ВОИС	Всемирная организация интеллектуальной собственности
ГА ООН	Генеральная Ассамблея Организации Объединенных Наций
ГООНВР	Группа Организации Объединенных Наций по вопросам развития
ГПК	Глобальная программа кибербезопасности (МСЭ)
ГПЭ	Группа правительственных экспертов
ГПЭ ООН	Группа правительственных экспертов Организации Объединенных Наций
Европол	Европейское полицейское ведомство
ЕС	Европейский союз
ИКТ	Информационно-коммуникационные технологии
ИМПАКТ	Международное многостороннее партнерство против киберугроз (Малайзия)
ИСО	Международная организация по стандартизации
ИТ	Информационные технологии
КВУП	Комитет высокого уровня по программам
КВУУ	Комитет высокого уровня по вопросам управления
КСР	Координационный совет руководителей
КЦД	Конфиденциальность, целостность и доступность
МАГАТЭ	Международное агентство по атомной энергии
МСЭ	Международный союз электросвязи
МСЭ-HLEG	Группа экспертов высокого уровня Международного союза электросвязи
МЭК	Международная электротехническая комиссия

НАТО	Организация Североатлантического договора
НРС	Наименее развитые страны
ОАЭ	Объединенные Арабские Эмираты
ОБСЕ	Организация по безопасности и сотрудничеству в Европе
ОМУ	Оружие массового уничтожения
ООН	Организация Объединенных Наций
ПРООН	Программа развития Организации Объединенных Наций
ПУИ	Поставщик услуг интернета
СБСЕ	Совещание по безопасности и сотрудничеству в Европе
СЕ	Совет Европы
СЕФАКТООН	Центр Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям/Европейская экономическая комиссия Организации Объединенных Наций
СОРМ	Система технических средств по обеспечению оперативно-розыскных мероприятий
ФБР	Федеральное бюро расследований
ФУИ	Форум по вопросам управления использованием интернета
ЦЕРН	Европейская организация ядерных исследований
ЭСКАТО	Экономическая и социальная комиссия Организации Объединенных Наций для Азии и Тихого океана
ЭСКЗА ООН	Экономическая и социальная комиссия Организации Объединенных Наций для Западной Азии
ЮНЕСКО	Организация Объединенных Наций по вопросам образования, науки и культуры
ЮНИДИР	Институт Организации Объединенных Наций по исследованию проблем разоружения
ЮНКТАД	Конференция Организации Объединенных Наций по торговле и развитию
ЮНОДК	Управление Организации Объединенных Наций по наркотикам и преступности

Контактная информация:
Международный союз электросвязи
Place des Nations – CH-1211 Geneva 20
Switzerland
E-mail: cybersecurity@itu.int
Website: www.itu.int/cybersecurity

ISBN 978-92-61-15304-5

Отпечатано в Швейцарии
Женева, 2015 г.

Фотографии представлены: Shutterstock

11/2014