DOI 10.37882/2223-2974.2020.11-2.15

СПАМ: МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ

SPAM: INTERNATIONAL-LEGAL ASPECTS

Rastegari Sayedebrahim

Summary: Mass emailing of unwanted messages has become a huge issue in the area of the Internet and electronic communications. The problem of spam does not mainly refer to the content of the message, but to the user's consent to receive them. Due to the fundamental limitlessness of the Internet, the effective struggle against spam is not possible under the federal legislation. This article considers the problem of spam in the context of federal and international law in order to clarify the need for the International Corporation for the fight against spam.

Keywords: spam, internet, international law, security, email.

Растегари Сайедэбрахим
Аспирант, Санкт-Петербургский государственный университет, Санкт-Петербург
ebrahimrastegari@gmail.com

Аннотация: Массовая рассылка нежелательных сообщений стала огромной проблемой в сфере сети Интернет и электронной коммуникации. Проблема спама заключается не столько в содержании сообщений, сколько в согласии на их получение. В силу принципиальной безграничности Интернета эффективная борьба со спамом невозможна в рамках федерального законодательства. В данной статье рассматривается проблема электронного спама в контексте федерального и международного права с целью разъяснения потребности в Международной корпорации по борьбе со спамом.

Ключевые слова: спам, интернет, международное право, защита, электронная почта.

Введение

Спам – системная отправка нежелательных массовых электронных сообщений при помощи электронных систем обмена сообщениями. «Спам – это такой жизненный факт, с которым сталкивается почти каждый пользователь электронной почты, - писал Х. Ньюман, - некоторые разработчики Web-страниц говорят, что более половины трафика их компьютеров приходится на спам».

Принято выделять несколько типов спама в зависимости от получателя: первый тип – спам системы телеконференций сети Интернет, который не всегда может быть отозван и посылает сообщение многочисленной группе людей, читающей RSS-ленту – электронную доску объявлений. Второй тип – это почтовый спам. Третий тип спама – телефонные сообщения, как голосовые, так и в СМС. И четвертый тип спама – когда отправляют письма владельцам сайтов с помощью формы обратной связи на сайте.

Почтовый спам, также известный как нежелательные массовые электронные сообщения (англ. unsolicited bulk e-mail – UBE), представляет собой практически идентичные сообщения, отправленные многочисленным получателям посредством электронной почты [1]. Спам любого типа обладает следующими признаками: массовость рассылки и несогласованность с получателем. Данные получателя спамеры приобретают различными способами: поиск в открытых источниках, переход пользователем по ссылке, указанной в письме.

Несмотря на то, что первый случай отправки почтового спама задокументирован в 1978 году, изучение данной проблемы в научной литературе началось лишь с 1982 года. Одна из первых работ, где рассматривается данная проблема – статья Питера Дж. Деннинга. Приблизительно 95% содержащих спам сообщений отправляется ботами.

Так как спам является причиной многочисленных перегрузок системы, он представляет собой проблему не только для получателей, но и для всей инфраструктуры всемирной сети. Соответственно, для решения данной проблемы необходимо сотрудничество работоспособных профессионалов, специализирующихся каждый в различных областях знаний. К таким профессионалам относятся:

1. законодатели и общественные контролирующие органы как официальные лица, защищающие частную жизнь и информацию;
2. правоохранительные органы;
3. интернет-провайдеры и провайдеры почтовых сервисов;
4. операторы хостингов;
5. организации, ответственные за обучение маркетологов в Интернет-сфере;
6. организации, представляющие Интернет-пользователей;
7. предприятия частного сектора, занимающиеся фильтрацией спама или борющиеся с «фишингом».

Безграничность Интернета – причина создания законов против спама на национальном и международном уровне. Развитые страны начали исследовать механизм международного сотрудничества по вопросу почтового регулирования и международного контроля в качестве ответной реакции на огромное количество спама. Были созданы двусторонние и многосторонние декларации и

меморандумы о взаимодействии, но упомянутые договоры не стали эффективными из-за того, что они не были юридически обязательными. Борьба со спамом включает множество правовых аспектов, включая политику коммуникации, торговлю и конкуренцию, конституционную гарантию свободы слова и неприкосновенности частной жизни, защиту потребителей и идентификацию преступлений.

Интернет в контексте прав человека

Так как одновременно с прогрессом информационных технологий растет количество пользователей всемирной сети, защита их прав является важнейшим юридическим вопросом, а построение информационного общества становится одной из глобальных проблем нового тысячелетия [2].

Стокгольмское совещание экспертов по правам человека (2010 г.) можно считать логическим началом для анализа взаимоотношений между информационными технологиями и правами человека. Международные стандарты прав человека и их ограничения, согласно общему мнению ученых-правоведов, являются необходимым условием свободы самовыражения. Первая Всемирная встреча на высшем уровне по вопросам информационного общества (ВСИО), проведенная в декабре 2003 г., также признала взаимосвязь между информационными технологиями и правами человека посредством принятия Декларации принципов, своего рода «конституции для киберпространства», которая призвала к тому, чтобы развитие информационного общества соответствовало признанным стандартам прав человека [3]. Всеобщая декларация прав человека, принятая ООН в 1948 году, рассматривается как оптимальная база для анализа проблемы взаимосвязи Интернета и прав человека. Например, все те принципы, что обеспечили запрет на дискриминацию в любом ее проявлении можно в разнообразных ситуациях так же отнести и к миру цифровых технологий. Уважение человеческого достоинства и равные права означают, в первую очередь, равный доступ к Интернету и информационным активам. «Онлайн» дискриминация по политическому, религиозному или половому признаку в этом случае препятствует осуществлению права на свободу самовыражения.

На второй сессии Всемирного Саммита по вопросу об информационном обществе (ВСИО) в Тунисе в 2005 году обсуждалась проблема регулирования сети Интернет и был составлен заключительный документ «Тунисские программа для информационного общества», который был принят Международным союзом электросвязи (МСЭ), но он не был юридически обязательным [4]. Сегодня важность проблемы спама в мире состоит в том, что посредством спама распространяются черви, вирусы, и трояны и прочие формы мошенничества непосредственно финансовой природы и идентифицирующиеся как потенциальная угроза использованию сети Интернет и электронной почты.

Законы о спаме в мире

После того как первый закон против спама был принят в 1997 году в США в штате Невада, около 75 мировых правительств приняли собственные законы против спама.

Первый Федеральный закон против спама появился в 2003 году в США (CAN-SPAM – Controlling the Assault of Non-Solicited Pornography and Marketing Act). В дальнейшем аналогичные законы приняли Австралия в 2003 году, Канада, Китай в 2006 году и Израиль в 2008 году.

В апреле 2004 года было учреждено Управление по связи и средствам массовой информации Австралии для регулирования законодательства против спама. Закон 2003 г. «О спаме» обеспечивает гражданские и административные полномочия для запрета отправки незапрашиваемого коммерческого электронного письма. Закон использует систему «опт-ина» (рассылка по подписке) и требует, чтобы коммерческие электронные сообщения включали указание на личность отправителя и возможность отказаться от рассылки. Закон 2003 г. «О спаме» дает предпосылку для вступления в законную силу международных конвенций против спама. К данному моменту Австралия уже вступила в международные соглашения с Великобританией, США, Кореей и Таиландом.

Норвегия одной из первых приняла поправки к закону «Об управлении маркетингом», который установил режим «опт-ина» [5]. Осенью 2004 года Чешская Республика разработала для спама определенное законодательство в форме закона «О надежности информации общественных сервисов».

В сентябре 2004 года Финляндия приняла закон «О защите данных в электронных средствах связи». Закон осуществляет Директиву 2002/58/ЕС Еврокомиссии относительно спама (Директива по частной жизни и электронным средствам связи), а также дает Интернет-провайдерам право блокировать спам при определенных обстоятельствах без согласия получателя [6]. Согласно этой же директиве, Дания провела закон «О маркетинговых практиках», который установил «опт-иновую» схему. В июне 2004 года Франция ввела закон «О доверии в цифровой экономике» (Loi pour la confiance en l'économique numérique), который ввел «опт-иновый» режим для физических лиц и осуществил Директиву 2002/58/ЕС. Нидерланды реализовали данную Директиву посредством закона «О широковещании», который установил «опт-ин» режим. Закон требует идентификации отправителя и предоставления возможности отказаться от рассыл-

ки. Голландский закон «О защите личных данных» также обеспечивает некоторую защиту против спама.

Великобритания для борьбы со спамом ввела инструкции по «Частной жизни и электронным средствам связи» (Директива ЕС) в 2003 году. Инструкции обеспечивают «опт-ин» режим для физических лиц, но согласия на рассылку достаточно, чтобы сообщение не считалось спамом. Однако в письме должен быть указан реальный адрес электронной почты, чтобы получатели могли отправить запросы на отказ от рассылки.

Япония приняла закон «О регулировании передачи специальной электронной почты». Закон устанавливает режим «опт-аута» (рассылка без запроса получателя), но требует идентификации отправителя и предоставления инструкций по отказу от рассылки.

Законы Южной Кореи, так же предполагая режим «опт-аут», требуют, чтобы коммерческие сообщения содержали личность их отправителя и предоставляли возможность отказаться от рассылки.

Можно назвать несколько примеров таких подходов, выработанных благодаря международному сотрудничеству: Набор методов борьбы со спамом ОЭСР (2004 г.), Принципы АТЭС для действий против спама (2005 г.), Соглашение Африканского союза по кибер-законодательству в Африке, Африканская экономическая комиссия ООН (2012 г.), Тунисский План действий с Саммита Мира ООН по вопросу об информационном обществе (2005 г.), Резолюция 50-ти Мировых телекоммуникационных ассамблей стандартизации, подписанная МСЭ (2004 г.), CAPTEF (Conférence des administrations des postes et des télécommunications d'expression française – Французская конференция администраций почтовых служб и служб связи), а также лондонский План действий по международному сотрудничеству в борьбе против спама, подписанный 27 странами в октябре 2004 г. Кроме того, девятнадцать франкоговорящих африканских стран приняли Декларацию по борьбе со спамом 30 марта 2005 г. Государства-члены Азиатско-тихоокеанского союза (Австралия, Китай, Япония, Корея, Китай, Малайзия и некоторые другие ассоциации и организации) признали важность борьбы со спамом и приняли «Сеульско-мельбурнский меморандум о взаимопонимании в вопросах многостороннего сотрудничества в борьбе против спама» в 2007 году. Однако, в сущности, выработка вышеуказанных подходов не привела к созданию международных правовых норм об Интернет-регулировании, и принятые договоры не были юридически обязательными.

Технические методы борьбы со спамом

Осознавая общественную опасность спама, ряд государств принял законы, связанные с ограничением или запрещением незапрашиваемых массовых почтовых рассылок коммерческого или некоммерческого содержания. Угрозой национальной безопасности страны является отправка письма с политическим или религиозным содержанием, вирусными программами и другими формами действий хакеров, отправка частной информации другим людям с целью дискредитации права на неприкосновенность частной жизни, средств связи, безопасности телефона, почты и других форм связи.

В ходе рассмотрения многих установленных национальными законодательствами методов было выявлено, что большая часть из них состоит из создания брандмауэров в среде передачи данных между ключевыми зонами доверия сети Интернет. Китайская Народная Республика была в числе первых стран, внедривших национальную систему фильтрации. Эта система известна как проект «Золотой щит» (неофициальное название — «Великий китайский фаервол» (англ. Great Firewall of China — игра слов, производное от англ. Great Wall of China — Великая Китайская стена). Этот проект считается образцом Интернет-цензуры и первого поколения методов Интернет-контроля.

Google внедрил систему определения ботов – Recaptcha, когда требуется выполнить определенные действия, чтобы отправить сообщение [7]. На сайтах CMS используют плагины-антиспам.

Актуализация таких тем, как терроризм, детская порнография и кибер-безопасность способствовали росту ожиданий государственного регулирования киберпространства, и, в частности, оградить граждан от нежелательного контента. Как ни парадоксально, развитые демократические государства в Организации по безопасности и сотрудничеству в Европе (ОБСЕ) — включая членов Европейского союза (ЕС) — (возможно, неумышленно) сделали первый шаг к учреждению глобальной нормы по фильтрации политического контента. Они внесли предложение подвергнуть цензуре контент, имеющий целью вызвать ненависть к лицам и группам лиц по признаку расы, религии, пола, сексуальной ориентации, национального происхождения и иным признакам. Одновременно с этим движение к свободе информации в развивающихся странах началось с конца XX – начала XXI века. Среди этих стран южноафриканские страны (1996 г.), Южная Корея (1996 г.), Пакистан (2002 г.). Кроме того, одни страны полностью отделились от глобальной сети, а другие (например, США) накладывают минимальное ограничение на информационный доступ.

Заключение

Спустя год после того, как прошла Тематическая встреча ВСИО по мерам противодействия спаму, МСЭ продолжает свои усилия в борьбе со спамом, призывая

на помощь все стороны, заинтересованные в «ВСИО. Тематическая встреча по кибербезопасности». К сожалению, спам по-прежнему является серьезной межотраслевой международной проблемой, которая не только растет в объеме, но и изменяет свою природу. Эта проблема требует ликвидации за счет скоординированных действий всех сторон, заинтересованных в создании и поддержании информационного общества.

Ключевой урок, который можно извлечь из рассмотрения опыта ведущих стран в борьбе со спамом, заключается в том, что введение законодательства против спама не является панацеей. Для значительного продвижения в разрешении международной проблемы спама необходимо проявить гибкость и разносторонний подход, что требует значительных временных и ресурсных вложений.

Несмотря на важность исследования международного опыта, следует учесть, что даже самые эффективные методы борьбы со спамом не универсальны. Каждая страна функционирует в своей уникальной области с точки зрения ее отличных конституционных и правовых рамок и различных типов контролирующих органов. Соответственно, необходим дальнейший анализ, чтобы понять, какой метод приведет к оптимальным результатам в каждой конкретной стране.

ЛИТЕРАТУРА

1. RIPE NSS Good Practice For Combating Unsolicited Bulk Email // https://www.ripe.net/publications/docs/ripe-206 (дата обращения 28.10.2020).
2. Document WSIS-03/GENEVA/DOC/4-E // http://www.itu.int/net/wsis/docs/geneva/official/dop.html (дата обращения 28.10.2020).
3. ЮНЕСКО между двумя этапами Всемирного саммита по информационному обществу: Итоговый документ международной конференции. М.: Институт развития информационного общества, 2005.
4. Тунисская программа для информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R// https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения 28.10.2020).
5. Ельчанинова Н.Б. Правовые методы борьбы со спамом // Известия ЮФУ. Технические науки. 2008. № 10 (87).
6. Директива Европейского Парламента и Совета Европейского Союза (Директива о конфиденциальности и электронных средствах связи) // https://pd.rkn.gov.ru/docs/Direktiva_Evropejskogo_Parlamenta_i_Soveta_Evropejskogo_Sojuza_200258ES_ot_12_ijulja_2002.pdf (дата обращения 29.10.2020).
7. Google Developer's Guide Introduction // https://developers.google.com/recaptcha/intro (дата обращения 29.10.2020).

Журнал «Современная наука: актуальные проблемы теории и практики»

Санкт петербургский государственный университет