

А. И. А ф о н и н

**ПРАВОВОЕ РЕГУЛИРОВАНИЕ ВЕДЕНИЯ
АДРЕСНЫХ БАЗ ДАННЫХ СЕРВИСА
ЭЛЕКТРОННОЙ ПОЧТЫ**

Рассмотрены вопросы законодательного регулирования методов, способов и технологий формирования баз данных адресов потенциальных получателей электронных сообщений.

Обязательным условием рассылки сообщений в сервисе электронной почты является наличие базы (пакета) электронных адресов получателей. Такие базы формируются путем сбора адресов из общедоступных источников, например средств массовой информации, и источников, доступ к которым ограничен в соответствии с законом.

В первом случае речь идет о легитимных способах сбора в целях последующего таргетинга¹. Таргетинг с использованием электронной почты предполагает семантическую обработку следующих данных пользователей адресов: юридический статус получателя (юридическое или физическое лицо); местонахождение (населенный пункт, регион, страна); вид деятельности организации или интересы пользователей; уровень доходов, образование, возраст, пол и т.д.

Такая обработка может проводиться только “ручным” способом, и именно поэтому адреса собираются, как правило, из общедоступных источников.

Очевидно, что подобные методы неприемлемы для рассылки сообщений, цель которой — распространить незапрошенную информацию максимально возможному неопределенному кругу лиц (спаминг [1]). С одной стороны, такой подход предполагает высокую экономическую эффективность рассылки, которая достигается благодаря массовому (в десятки тысяч адресов) распространению незапрошенных получателями электронных сообщений. С другой стороны, поступление спам-сообщений, как правило, сопряжено с причинением того или иного вреда получателю [2].

Антагонистические интересы отправителей и получателей спама обуславливают постоянное совершенствование спам-технологий в части разработки и применения специальных приемов, направленных

¹Таргетинг (англ. *target* — цель) — механизм, позволяющий выделить из всей имеющейся аудитории только ту часть, которая удовлетворяет заданным критериям (целевую аудиторию).

на повышение эффективности спаминга и преодоление противодействия Интернет-сообщества незапрошенным рассылкам электронных сообщений.

Описанная ситуация характерна, прежде всего, для процесса формирования баз данных спам-адресов. Для целей спаминга адреса обычно получают из источников, доступ к которым ограничен, одним из следующих методов².

1. *Атаки со словарем.* При использовании этого метода сообщения направляются по случайным адресам, которые формируются из данных электронных словарей: собственных имен, имен с добавлением цифр, обычных сочетаний имени и фамилии, распространенных сочетаний слов и цифр, а также путем перебора простых коротких сочетаний и т.п. Возвращение сообщения означает, что адрес не существует.

2. *Метод аналогий.* При наличии у отправителя какого-либо адреса возможна проверка существования близких, производных или аналогичным образом составленных адресов. Существующие спам-листы позволяют также провести сканирование всего домена на наличие других адресов.

3. *Сканирование специальными программами Интернет-пространства* (web-сайтов, форумов, чатов, досок объявлений, Usenet News, баз данных Whois) в целях поиска случайным образом на web-страницах символов “@”.

4. *Несанкционированное копирование баз данных сервисов, операторов связи* и т.п. Кроме адресов, в этом случае достаточно часто появляется дополнительная информация (персональные данные) об адресате, которая позволяет создавать тематические базы данных.

5. *Несанкционированный доступ к персональным данным адресатов*, включая адресные книги почтовых клиентов, посредством компьютерных вирусов и прочих вредоносных программ.

Следует отметить, что при использовании первых трех методов невозможно получить какие-либо данные о получателе сообщения (важных для таргетинга), кроме его электронного адреса.

Таким образом, в связи с тем, что наличие адреса, с одной стороны, является обязательным условием рассылки электронных сообщений, а, с другой стороны, способы их получения могут нарушать права пользователей электронной почты, правовое регулирование такого рода отношений является необходимым и приобретает принципиальное значение.

²Перечень методов неисчерпывающий; приводится по материалам различных Интернет-сайтов.

В июле 2006 г. принят федеральный закон № 149-ФЗ “Об информации, информационных технологиях и о защите информации”, заменивший ранее действовавший закон “Об информации, информатизации и о защите информации”. В новом законе предпринята попытка регулирования отношений в информационно-телекоммуникационных сетях, к которым, исходя из определения закона, можно отнести Интернет-сервис электронной почты.

В частности, в п. 3 ст. 10 закона установлено, что “при использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации”.

В этой связи представляется полезным оценить перспективы регулирования процедуры “определение получателей информации”. Прежде всего, отметим, что в упомянутой статье использованный законодателем термин “определять” не имеет ни легитимной, ни устоявшейся в Интернет-сообществе семантики. Поэтому можно предположить, что он охватывает и процедуру формирования баз данных адресов получателей информации.

Таким образом, вновь принятый закон однозначно показывает, что в российском обществе существует понимание необходимости законодательного регулирования методов, способов, технологий формирования баз данных адресов потенциальных получателей электронных сообщений.

Однако описанные и широко применяемые в настоящее время способы получения адресов могут нарушать права пользователей электронной почты, поскольку сведения об абонентах и их почтовых адресах являются конфиденциальной информацией и подлежат защите в соответствии с законодательством РФ (федеральные законы “Об информации, информационных технологиях и о защите информации”, “О персональных данных”, “О связи” и УК РФ).

Теоретически возможно легитимное получение адресов через web-форму, подписного робота и т.п. Но в этом случае включение адреса в список, по которому проводится рассылка, строго говоря, может допускаться лишь при наличии надлежащей технической процедуры подтверждения подписки. Эта процедура должна гарантировать соответствующее волеизъявление пользователя адреса и исключать возможность попадания адреса в список рассылки (единичной или регулярной) по инициативе третьих лиц.

Следует отметить, что в настоящее время единственной технологией, удовлетворяющей приведенным требованиям, является технология цифровой подписи. Однако в силу многих причин, обсуждение

которых выходит за рамки настоящей статьи, ее широкое применение в сервисе электронной почты пока невозможно. Но в этом случае основным ограничивающим фактором формирования массовых баз данных, на наш взгляд, является снижение экономической эффективности, обусловленное офф-лайнным режимом подтверждения подписки. Поэтому, как представляется, корректный с точки зрения закона механизм “определения” получателей не будет востребован пользователями Интернета, специализирующимися на создании баз данных для распространения электронных сообщений.

Еще один важный аспект исследуемого вопроса вызывает неоднозначное понимание: на процедуру “определение” потенциального получателя сообщения в законе введено единственное ограничение — обязанность предоставления получателю возможности отказа от распространения информации.

Нечеткая, на наш взгляд, формулировка исследуемой нормы может породить проблемные ситуации в правоприменении. Так, указанное условие обосновано и работоспособно лишь при распространении информации “по подписке”. Но при распространении незапрошенной получателем информации наличие возможности отказа от ее получения не исключает как минимум однократного нарушения права адресата на получение только востребованной информации.

По этой причине предполагаемая законом возможность отказа подписчика от рассылки сама по себе не может служить основанием внесения адреса в базу помимо воли их пользователей. При этом соответствующее волеизъявление, как было указано ранее, нуждается в юридически значимом документировании.

Еще один аспект правового регулирования процедуры “определение” получателей сообщения проявляется при соотношении п. 3 ст. 10 Федерального закона “Об информации, информационных технологиях и о защите информации” с федеральным законом № 38-ФЗ “О рекламе”. Дело в том, что формирование массовых баз адресных данных необходимо, как правило, для осуществления рекламной деятельности в виде автоматического распространения рекламной информации по сетям электросвязи. Но закон “О рекламе” допускает использование сетей электросвязи для распространения рекламы только “при условии предварительного согласия абонента или адресата на получение рекламы” (п. 1 ст. 18) и ничего не говорит о механизме отказа от получения сообщений. В п. 2 ст. 18 закона вообще исключена автоматическая (без участия человека) рассылка сообщений и, тем самым, прагматика формирования массовых баз данных.

Проведенный сравнительный анализ действующего законодательства и вновь принятого закона “Об информации, информационных

технологиях и о защите информации” показывает, что в части регулирования процедур формирования и использования баз данных адресов получателей электронных сообщений имеется терминологическое, логическое и семантическое несоответствие.

Тем не менее, можно сделать вывод, что ведение массовых баз данных адресов получателей электронных сообщений является не соответствующим закону как в части сбора адресов рассмотренными выше (и аналогичными им) методами, так и в части их практического использования.

Таким образом, попытка законодательного урегулирования процедуры сбора и использования адресов на основе Интернет-технологий, являясь ответом законодателя на реальные потребности Интернет-сообщества, должна иметь дальнейшее развитие. Прежде всего, видимо, могут быть нормативно определены соответствующие правила ведения адресных баз данных и предусмотрена ответственность за их нарушение.

Однако исследуемая проблема значительно сложнее, чем простое декларирование необходимости установления правил сбора и использования адресов. Поэтому указанная нормотворческая деятельность должна протекать в рамках реализации комплекса мер по совершенствованию правового обеспечения противодействия спамингу.

СПИСОК ЛИТЕРАТУРЫ

1. Афонин А. И., Карпычев В. Ю. Технологические признаки спаминга // Материалы XIV науч.-техн. конф. “Системы безопасности”. – М.: Академия ГПС МЧС России, 2005. – С. 25–27.
2. Афонин А. И. Вред – как одно из последствий спаминга // Материалы XIV науч.-техн. конф. “Системы безопасности”. – М.: Академия ГПС МЧС России, 2005. – С. 28–30.
3. Афонин А. И. Концепция правового обеспечения противодействия спамингу / Труды VII междунар. симпозиума “Интеллектуальные системы”. – Краснодар, 26–30 июня 2006 г. – С. 358–361.

Статья поступила в редакцию 12.09.2006

Александр Иванович Афонин родился в 1953 г., окончил МВТУ им. Н.Э. Баумана в 1978 г. Проректор по безопасности МГТУ им. Н.Э. Баумана. Академик Академии проблем обороны, безопасности и правопорядка. Автор 9 научных работ в области информационной безопасности.

A.I. Afonin (b. 1953) graduated from the Bauman Moscow Higher Technical School in 1978. Vice-rector on security of the Bauman Moscow State Technical University. Academician of the Academy for Problems of Defense, Security and Law-and-order. Author of 9 publications in the field of information security.