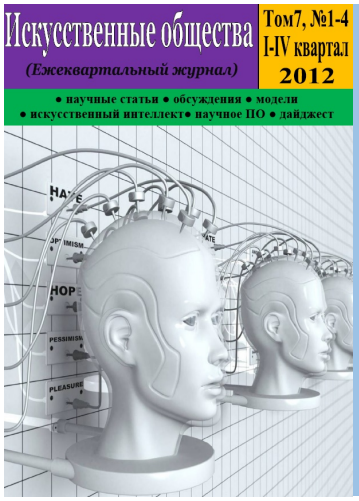

Artificial societies. 2013-2020

ISSN 2077-5180

URL - http://artsoc.jes.su

Issue 1-4 Volume 7. 2012

Risk of using of social networks

I. Bobkova
Associate Professor, GAUGN
Russian Federation, Moscow,

Abstract

The possible problems and risks in using social networks were studied and classified in order to minimize the negative effects for users of social networks. Social networks – the most dynamic of developing Internet sectors. Every year the army of social networks users is rising for millions. But analytics, users and owners of social networks have been thinking about risks and of this sector of Internet. An analysis of the problems reported by users of social networks, has identified the following risk groups: 1. Content risks - risks that are associated with the consumption of the information published in the Internet or in a network and includes any illegal or inappropriate content, which have a psychological impact, including materials that contain pornography, propaganda of extremism, drugs, gambling, religious sects, suicide, foul language, etc. 2. Communication risks - activities associated with interpersonal relationships of users, the possibility of being subjected to insults and attacks from other members of the community, including Illegal contact (grooming), cyber-bullying, etc. with tech-nology, finding victims through the network, planning crimes. 3. Electronic (cyber) risks - activity that involves the theft of personal information, making false pages and profiles, software, virus attacks, online - fraud, spam. 4. Consumer risks - consumer rights abuse, including distribution of substandard or counterfeit goods, theft of funds, the impact on potential customers through “friendly”, etc. 5. Using social networks for military and political purposes - both for espionage and disinformation, and for the information wars. 6. Dependence on social networks, which recognized by psychiatrists more seri-ous phenomenon than the dependence on computer games. Each user of the social network may suffer from a particular type of risk, so the greatest importance is the development of the individual measures to protect their profile in the network, familiarize children with the safety rules, the measures of net-work owners to improve security of its users, employers using the network as a pro-fessional should protect your company from possible damage, increase the security in social networks at the state level.

Keywords list (en): social networks, using of social networks, risks in using social networks

Date of publication: 30.11.2012

Citation link:

Bobkova I. Risk of using of social networks // Artificial societies. 2012. V. 7. Issue 1-4 [Electronic resource]. Access for registered users. URL: https://artsoc.jes.su/s207751800000046-9-1/ (circulation date: 23.09.2020).

1 Социальные сети на данном этапе - самый динамично развивающийся сектор Интернета. Каждый год количество пользователей социальных сетей увеличивается на десятки миллионов человек. Самую популярную мировую сеть Facebook посещает более 700 млн. пользователей в месяц. Но только в последние годы аналитики, пользователи и владельцы социальных сетей стали всерьез задумываться о рисках и опасностях этого сектора Интернета (1,2,3,6).

2 В результате анализа проблем, возникающих у пользователей социальных сетей, были выявлены следующие группы рисков:

3 1. Контентные риски – риски, которые связаны с потреблением информации, опубликованной в Интернете или в сети и включающей либо незаконное, либо неподобающее содержание, в т.ч. материалы, содержащие порнографию, пропаганду экстремизма, наркотиков, азартных игр, религиозных сект, суицида, нецензурную лексику, оказывающие психологическое воздействие и т.д.
2. Коммуникационные риски – деятельность, связанная с межличностными отношениями пользователей, возможность подвергнуться оскорблениям и нападкам со стороны др. членов сообщества, в т.ч. незаконные контакты (груминг), киберпреследования, кибербуллинг (агрессия в отношении более слабого лица) и т.п. с использованием информационных технологий, поиск жертв через сети, планируя уголовные преступления.
3. Электронные (кибер-) риски – деятельность, которая включает хищение персональной информации, создание ложных страниц и профилей, вредоносное программное обеспечение, вирусные атаки, онлайн - мошенничество, спам.
4. Потребительские риски – злоупотребление правами потребителя, в т.ч. распространение некачественной или контрафактной продукции, хищение средств, воздействие на потенциальных потребителей через дружеские контакты и т.п.
5. Использование социальных сетей в военных и политических целях – как для шпионажа и дезинформации, так и для информационных войн.
6. Зависимость от социальных сетей, которая признана психиатрами более серьезным явлением, чем зависимость от компьютерных игр.

4 Остановимся на отдельных, наиболее часто встречающихся рисках.

5 **1. Контентные риски**

6 Риски, которые связаны с потреблением информации, опубликованной в социальной сети, т.е. с ее негативным содержанием. Негативный контент бывает двух видов(2):

7 А) незаконный – это материалы, которые подпадают под определенные статьи УК, т.е. детская порнография (распространение, вовлечение и т.п.), наркотики (распространение, пропаганда и т.п.), азартные игры, все виды пропаганды религиозной, расовой или этнической вражды, в т.ч. вовлечение в террористические, экстремистские, фашистские организации и религиозные секты (о них следует сказать отдельно), преследование или агрессия (угрозы) по отношению к группе лиц или определенному человеку.

8 Б) неэтичный – это материалы, которые противоречат нормам морали и нравственности или социальным нормам, т.е. материалы, которые могут нанести вред психическому или моральному состоянию человека, особенно ребенку. Например, порнография (для взрослых), нецензурная брань, агрессия, пропаганда нездорового образа жизни (курение, пьянство, сексуальная распущенность, булемия), нанесение вреда здоровью (самоубийство, самоистязание, аудионаркотики и т.п.). К таким материалам относятся также те, которые позволяют манипулировать сознанием людей.

9 Особенно серьезную угрозу представляют эти проблемы в отношении детей. Детские риски при пользовании социальными сетями значительно выше аналогичных взрослых рисков в связи с высокой пользовательской активностью школьников, высоким уровнем бесконтрольности, ростом числа контентных и коммуникационных онлайн - рисков. У детей недостаточно опыта для того, чтобы реально оценить возможную опасность, поэтому они часто становятся жертвами преступлений. Чем старше школьники, тем слабее контроль взрослых: 70% учеников 9–10-ти лет и свыше 90% школьников старше 13-ти лет пользуются Интернетом, когда рядом нет родителей, учителей, других взрослых.

10 Сотрудниками Фонда Развития Интернет, факультета психологии МГУ им. М.В. Ломоносова и Федерального института развития образования Минобрнауки России в 2011 г. было проведено исследование "Дети России онлайн", в ходе которого в том числе был проведен опрос детей старше 11-ти лет о том, умеют ли они безопасно пользоваться социальными сетями (7).

11 Первые же опросы показали, как часто дети выкладывают в сеть полную информацию о себе (55% опрошенных), значительно облегчая дальнейшую работу злоумышленников. При этом менее половины умеют выполнять какие-либо действия, защищающие их во время работы в сети (сравнивать сайты для оценки достоверности информации, изменять настройки профиля в социальной сети, блокировать сообщения от кого-либо, уничтожать историю переписки, добавлять сайт в закладки, изменять настройки фильтра и находить информацию о безопасном пользовании Интернетом).

12

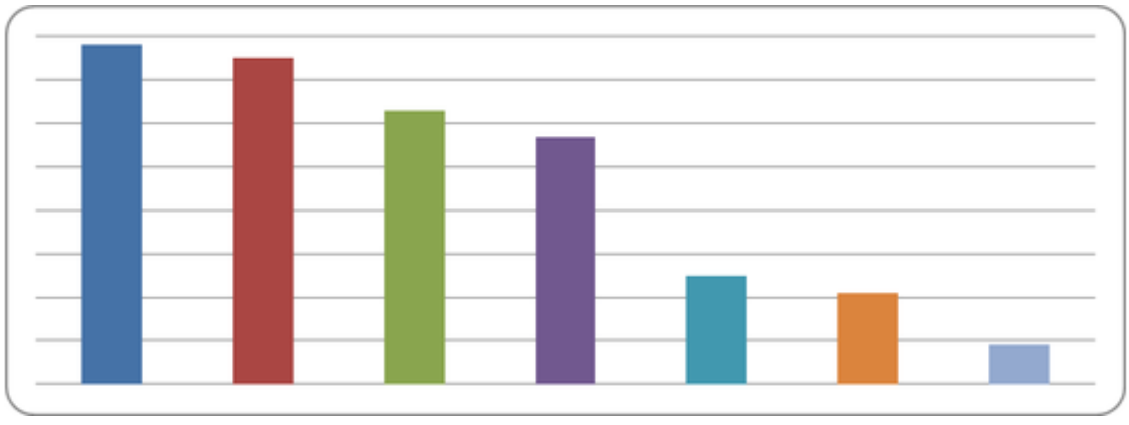

Рис.1. Персональная информация, выложенная в социальной сети, детьми старше 11 лет (негатив). Источник: Данные исследования "Дети России онлайн"

13

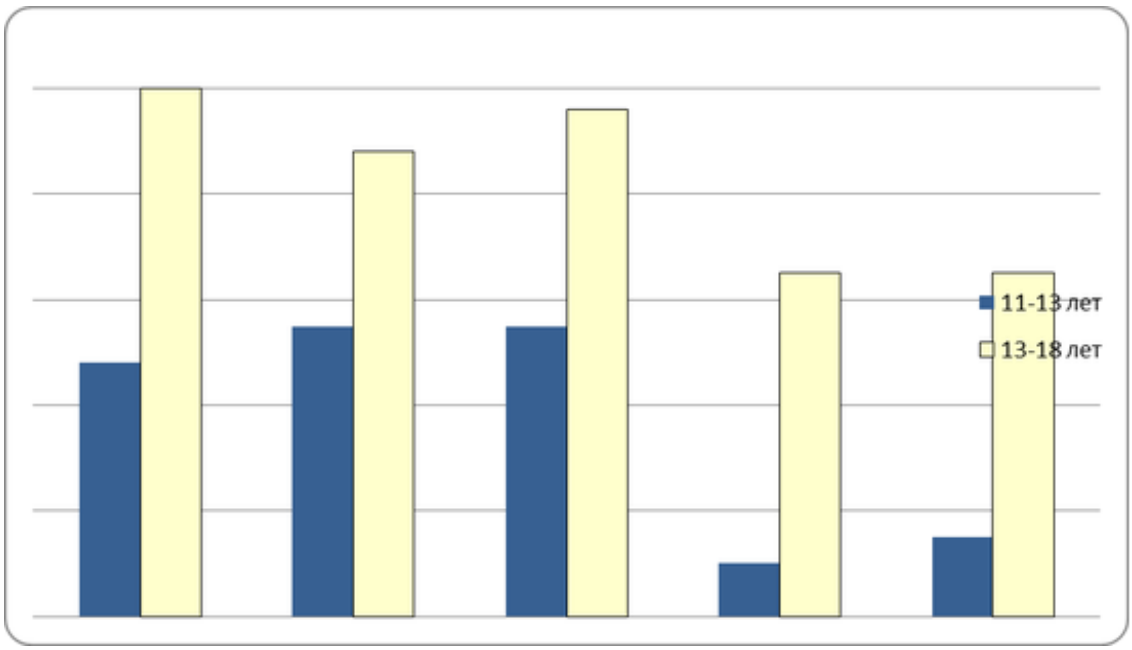

*Рис. 2. Навыки детей и подростков при работе в социальных сетях (позитив). Источник: Данные исследования "Дети России онлайн" Примечание: *- умеют выполнять хотя бы одно действие по обеспечению безопасности при работе в социальной сети*

14 Молодые люди обычно не понимают, что все, что выкладывается в социальные сети, остается там навсегда. Комментарии и отметки на фотографиях остаются даже после удаления аккаунта, а иногда и сам аккаунт удалить нельзя. Через несколько лет тексты матерящегося подростка или высказывания о его взглядах или поступках могут стать причиной краха будущего успешного политика.

15 К контентным рискам относят и риски, связанные с терроризмом, экстремизмом, национализмом. Здесь можно выявить несколько направлений:

16 1. Экономический экстремизм - устранение конкуренции в предпринимательской деятельности, уничтожение компаний с помощью анти-рекламы в сетях и мошенничества
2. Политический экстремизм - деятельность лиц, создающих предпосылки для разрушения экономики, Вооруженных Сил, систем образования и здравоохранения России и использующих социальные сети для запугивания населения, морального давления, пропаганды насилия, подготовка революций и т.п. (весна 2011 г.-) (8)
3. Националистический экстремизм - направлен на развал многонациональных государств, утверждение господства коренной нации (борьба за Халистан в Индии, движение басков в Испании и др.) и т.п.
4. Религиозный экстремизм проявляется в нетерпимости к представителям других конфессий или жестком противоборстве в рамках одной конфессии, в использовании социальных сетей для организации религиозных сект, движений, привлечения фанатиков для уничтожения и избиения представителей др. религий. И социальные сети, и религиозные секты имеют общую черту: часто являются прибежищем для лиц с недостатком реального социального общения, не имеющими близких людей, внутренними противоречиями, комплексами, находящимися в состоянии стресса и т.п. Именно поэтому все чаще социальные сети стали использоваться деструктивными религиозными сектами и группами для «ловли человеческих душ».
5. Экологические экстремисты выступают против научно-технического прогресса вообще, считая, что ликвидация неблагоприятных в экологическом отношении

производств – единственно возможный путь улучшения качества окружающей среды, для чего используется дискредитация соответствующих предприятий путем распространения ложной информации, привлечения сторонников для диверсионной деятельности..

6. Духовный экстремизм отвергает опыт, достижения другой культуры, навязывает в качестве официальной идеологии определенные социальные, религиозные, этнические стандарты – такие сообщества можно найти практически во всех крупный социальных сетях.
7. Молодежный экстремизм выражается в пренебрежении к действующим в обществе правилам и нормам поведения. Так как он отличается от взрослого меньшей организованностью, то нередко за ним стоят взрослые, которым молодые люди доверяют и стремится подражать, а те используют это в своих целях (см. пп.1-6).

17 В сентябре 2010 г. прокуратура Петербурга даже направила в Смольный предложение о разработке за счет городского бюджета компьютерной программы, которая будет отслеживать экстремистские материалы в социальных сетях. Однако, городская администрация на инициативу прокуратуры не отреагировала (14).

18 **2. Коммуникационные риски**

19 Эта деятельность связана с межличностными отношениями пользователей, в т.ч. возможность подвергнуться оскорблениям и нападкам со стороны др. членов сообщества - незаконные контакты (груминг), киберпреследования, кибербуллинг и т.п. с использованием информационных технологий, поиск жертв через сети, планируя уголовные преступления (2,8).

20 А) Кибербуллинг – неоднократное умышленное агрессивное поведение (необязательно физическое), направленное против более слабого лица с целью его унижения. Это поведение чаще всего распространено в подростковой среде, поэтому дети в социальных сетях – основной объект кибербуллинга. Эта проблема особенно актуальна для пользователей социальных сетей 11-12 лет: почти 30% детей сталкиваются с оскорблениями чаще 1 раза в неделю (в Санкт-Петербурге – 35%). Настораживает, что в России по оценке разных экспертов жертв буллинга в два раза больше, чем в европейских странах (В России 12,5% опрошенных детей подверглись буллингу при личном контакте, 11,5% - кибер-буллингу, в ЕС – 13% и 5% соответственно). От 9 до 22% детей в возрасте 9-16 лет сталкивались с кибербуллингом ежедневно при заходе в социальную сеть, причем максимум приходится на возрастную группу 11-12 лет, а в среднем 49% детей (41-55% в разных возрастных группах) – иногда (7).

21

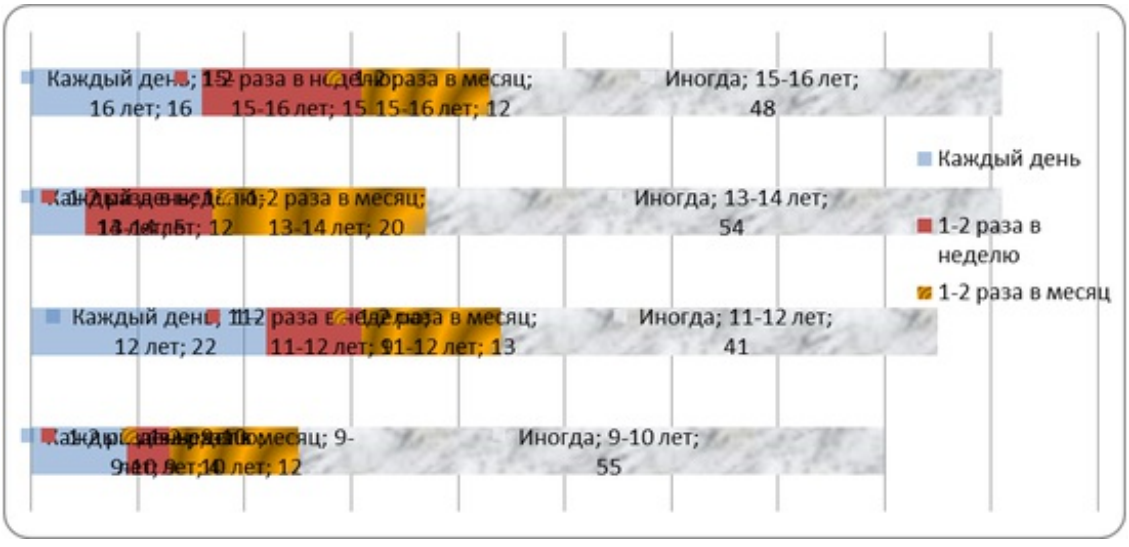

Рис 3. Частота столкновения с кибербуллингом в социальных сетях по возрастным группам. Источник: Данные службы психологической помощи «Дети онлайн».

22 Б) Груминг, или установление незаконных контактов Большое количество обращений в разные службы, так или иначе связанные со злоупотреблениями в социальных сетях – от администраторов этих сетей до служб психологической помощи и полиции, - связано с перепиской, в ходе которой злоумышленник пытается добиться контакта с жертвой в реальной жизни. Причем, 18 % звонков в службу психологической помощи – от родителей школьников. Схема проста: злоумышленник начинает общаться в социальной сети, представляясь ровесником ребенка, предлагают встретиться, а при отказе начинают оскорблять его или угрожать (груминг перерастает в буллинг). Избавиться от такого домогательства иногда получается только после привлечения полиции.

23 В) Мошенничество – злоупотребление доверием с целью получения выгоды. Причем, главное, что интересует преступников – информация (10,16,17).

24 Численность таких рисков в 2011 г. по сравнению с 2009 г. выросло почти вдвое. (Источник: опрос Associated Press и MTV).

25 - Специалисты компании "Доктор Веб" обнаружили новую мошенническую схему, жертвой которой уже стали многие пользователи социальной сети "ВКонтакте": получение пользователем сообщения с некоторой ссылкой от его «друга» из социальной сети – по ссылке пользователь перенаправляется на принадлежащий "Твиттеру" специализированный сервис - оттуда — на встроенное приложение, опубликованное на одной из страниц социальной сети "ВКонтакте". Созданное злоумышленниками приложение демонстрирует значок учетной записи жертвы и пояснение, сообщающее, что в интернете опубликован видеоролик с его участием. На этой же странице выводятся фальшивые комментарии пользователей из списка друзей жертвы. Жертве предлагается убрать ролик за соответствующее вознаграждение (Источник: http://www.belinter.net/security).

26 - «Сватовство» - обманутые невесты, познакомившиеся с мошенниками или сексуальными преступниками в социальных сетях, щедрые женихи, лишившиеся крупных денежных сумм, отправленных «на проезд» девушке к месту знакомства.

27 - В Великобритании страховщики подсчитали, что 12% всех краж в 2010 году было совершенно на основе информации из социальных сетей. Во-первых, адрес, фамилия, фото автомобиля и жены в шубке, детей в лагере в Великобритании и т.п. – все это поможет найти вору-домушнику любителя хвастаться своим материальным положением. Во-вторых, если пользователь каждый день появлялся в социальной сети в одно и то же время или рассказывает о предстоящем отъезде всей семьи на море, то легко установить, когда его квартира свободна. (Источник: http://bigcorp.ru)

28 - Запрашивание Интернет-магазинами избыточных конфиденциальных данных. Специалисты компанииий Symantec и социальной сети Профессионалы.ru провели совместный опрос среди пользователей интернет-магазинов. Наиболее часто запрашиваемой конфиденциальной информацией являются: телефон (81%) и домашний адрес (58%), дата рождения (43%), семейное положение (16%) и паспортные данные (16%). Согласно проведенному опросу, 33% пользователей расплачиваются с курьерами наличными, 53% - предоставляют магазинам электронной торговли свою личную информацию. По этим данным злоумышленники легко находят страничку пользователя в одной из популярных социальных сетей и подбирают жертву. (Источник: http://www.uniq-themes.ru/articles/opasnosti-socialnix-seteie.html)

29

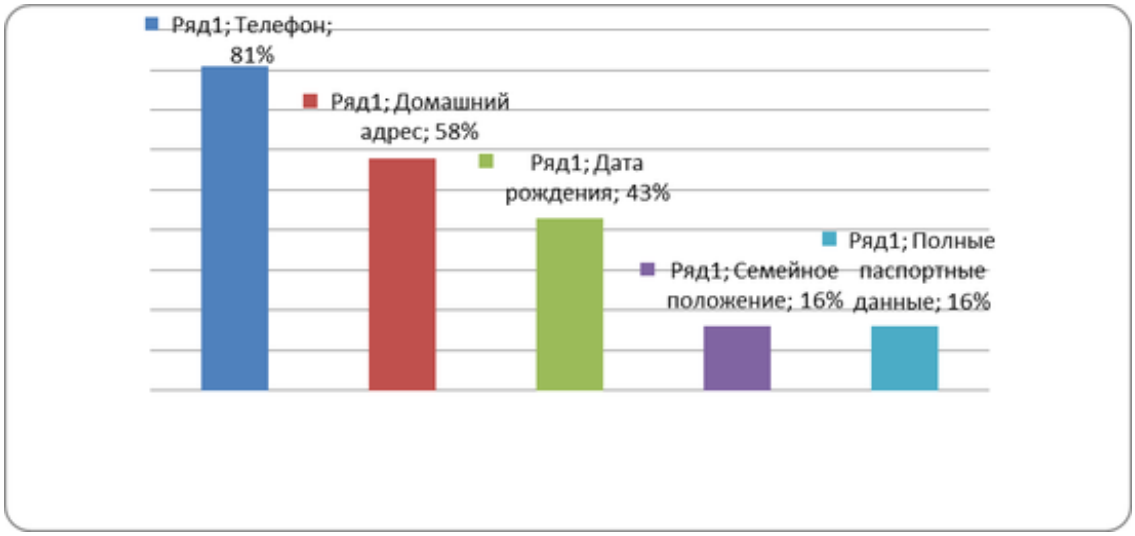

Рис 4. Данные, предоставляемые пользователями социальных сетей. Источник: Данные с сайта http://www.uniq-themes.ru

30 - Аферисты, цель которых та же информация о пользователе, но для того, чтобы он сам отдал свое имущество: уличные гадания (клиенту выдается информация из социальной сети, а дальше – «Позолоти ручку, всю правду скажу»), подбор жертвы, похожей на преступника по выложенным фотографиям (убийство или мошенничество с целью продажи квартиры или получения кредита по документам жертвы на основании внешнего сходства).

31 - Социальные сети, как оружие «зайцев» - с помощью сети Twitter обмениваются сообщениями о наличии или отсутствии контроллеров на определенных маршрутах. (в Гамбургском объединении «зайцев» - 6500 участников, в мюнхенском – более 13700 человек, в сети «ВКонтакте» крупнейшая из подобных групп насчитывает свыше 5800 участников желающих ездить без билета. (Источник: http://odnoklassniksi.ru/)

32 **3. Электронные (кибер-) риски**

33 Это самый распространенный вид деятельность, который включает хищение персональной информации, создание ложных страниц и профилей, вредоносное программное обеспечение, вирусные атаки, онлайн - мошенничество, спам (11,12,15).

34 Риски, связанные с социальными сетями делятся на три основные категории:

35 1. Риск взлома самой учетной записи в социальной сети.
2. Риск заражения пользователей вредоносным кодом на сайте социальных сетей.
3. Риск того, что хакер сможет получать информацию через сайт социальной сети, которая позволит ему осуществлять атаку на корпоративную сеть (социально-техническая атака).

36 *Взлом персональных страниц, аккаунтов.* Например, молодой человек оставляет компьютер включенным и незаблокированным, когда надолго оставляет его и выходит из комнаты, давая злоумышленнику возможность рыться в письмах или оставлять неприятное обновление статуса на странице владельца. В результате таких действий, двум третям столкнувшихся с этой проблемой пришлось менять пароли, 46% помимо паролей поменяли email адреса, имена в сети или телефонные номера, 25% пришлось удалять аккаунты.

37 *Компрометирующая информация о человеке,* к примеру фотографии или видео, выкладываются в свободный доступ, что может привести к тяжелым последствиям (в 2007

году в США тринадцатилетняя девочка после такого взлома покончила с собой) или пользователя завлекают на специальные сайты (с похожими на адрес соцсети адресами или предлагающие какие-то услуги), чтобы с их помощью получить пароли этого пользователя. (Источник: http://www.rosbalt.ru/style/2010)

38 *Спам в почтовом трафике* составляет, по исследованиям лаборатории Касперского, 78% и продолжает расти, из них 4,5% содержали вредоносные файлы. В списке 5 стран – основных мировых источников спама, распространяемого через социальные сети, в сентябре 2011 г. вошли Индия (14,1%), Бразилия (10,1%), Индонезия (9%), Южная Корея (7,3%) и Перу (4,9%). Россия в этом рейтинге, по сравнению с августом, сместилась на две позиции вниз и заняла 13 место (12).

39

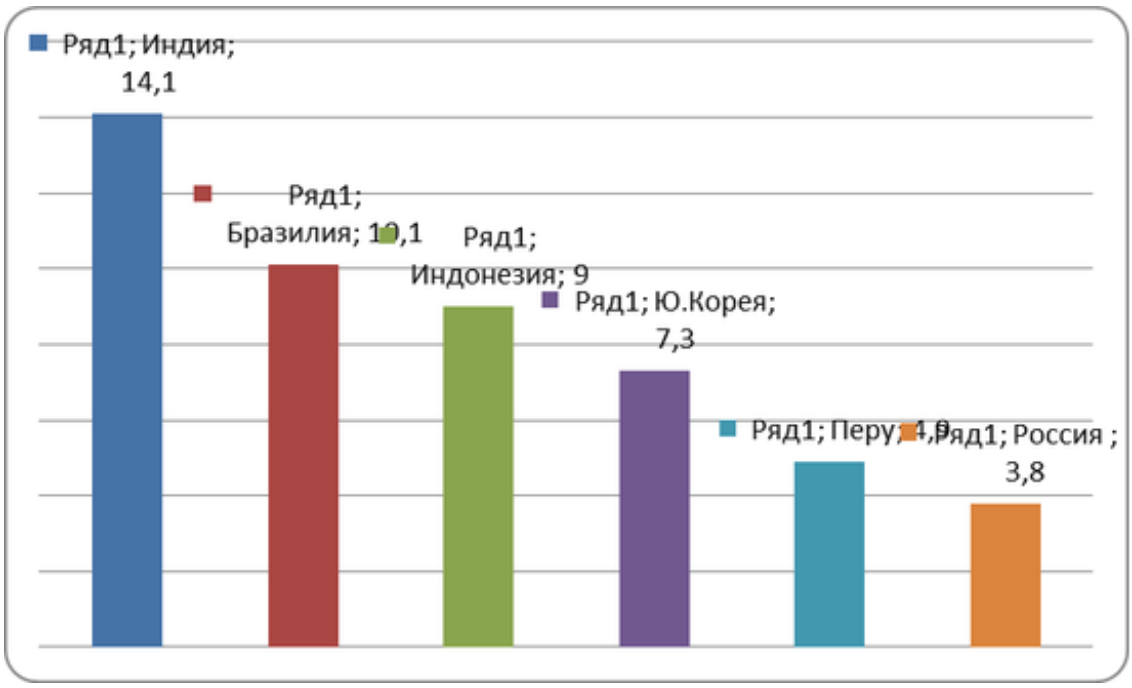

Рис. 5. Страны - основные источники мирового спама в почтовом трафике (в %). Источник: Данные лаборатории Касперского в сентябре 2011 г.

40 *Клонирование* - любой желающий может, считав конфиденциальные данные, от имени другого пользователя открыть страничку в любой социальной сети. Добавить туда информацию и фото из блогов. И двойник будет делать все, что пожелает его создатель: от распространения спама и порочащей информации до настоящих преступлений.

41 Facebook является наиболее частой причиной *заражения вредоносным ПО* и нарушения конфиденциальности. YouTube занял второе место по количеству заражения вредоносным ПО, в то время как Twitter явился причиной значительного количества нарушений конфиденциальности. Среди компаний, которые понесли финансовые потери из-за утечки данных, на первых местах те же социальные сети (11).

42

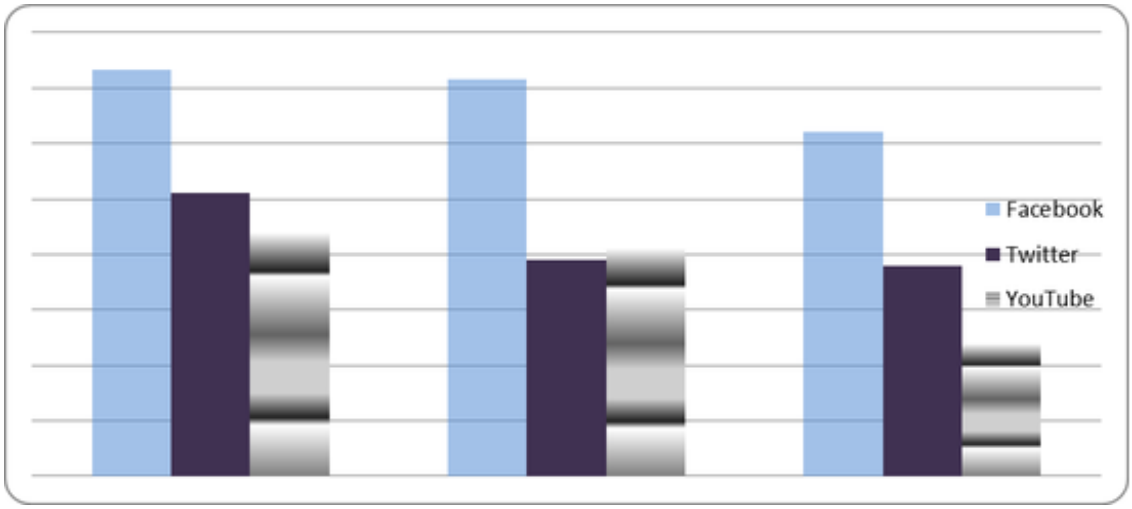

Рис 6. Кибер-риски крупнейших социальных сетей. Источник: Данные с сайта http://www.infosecurity.ru/_gazeta

43 **4. Потребительские риски**

44 Это злоупотребление правами потребителя, в т.ч. распространение некачественной или контрафактной продукции, хищение средств, воздействие на потенциальных потребителей через дружеские контакты и т.п.

45 В отдельную группу можно выделить потребительские риски, связанные с работодателями. Эти проблемы бывают двух видов.

46 А) со стороны работодателей(10,18)

47 - 78% крупных компаний используют социальные сети с целью рекламы и продвижения услуг и товаров на рынке.Специальные люди регистрируются в группах и сообществах, завоевывают там авторитет и понемногу продвигают свои идеи среди членов этих групп. Именно от этих людей зависит, станет ли новая марка популярна среди масс. Однако, если это делается слишком явно, российское социальное сообщество такую рекламу отвергает. (Источник: http://www.rosbalt.ru Entensys «Анализ использования Интернета офисными работниками»)

48 - каждый пятый британский работодатель регулярно использует социальные сети для поиска дополнительной информации о сотрудниках и изучения их личностных качеств (Исследование The Times). Российские работодатели это делают в исключительных случаях.

49 - информация, которую пользователь социальной сети сообщает о себе, может быть использована работодателем для давления на него или увольнения. Например, сотрудник корпорации Google после первого дня работы опубликовал в своем блоге, что первый рабочий день прошел, а он абсолютно ничего не делал, при этом зарплата все равно шла. На следующий день его уволили.

50 Б) для работодателей – типичные для пользователей, но с более разрушительными последствиями

51 - материальный ущерб

52 • трата времени сотрудниками. Группа сайтов «Социальные сети, персональные сайты и блоги» посещается 20,8% офисных работников в рабочее время, поэтому многие фирмы стали вводить запреты на использование социальных сетей (Источник: http://www.rosbalt.ru Entensys «Анализ использования Интернета офисными

работниками»)

- отсутствие конфиденциальности, т.к. в социальных сетях иногда публикуют данные о корпоративных финансах, бизнес-практике, рабочих процессах, которые могут быть использованы злоумышленниками против данной компании.
- дискредитация со стороны конкурентов в социальных сетях. В социальных сетях очень быстро распространяется негативная информация. Вычислить нанятого распространителя негатива и доказать факт клеветы достаточно сложно, да и опровержение информации до потребителя может не дойти.
- случайные или целенаправленные атаки, которым подвергаются сети предприятий из-за неосторожных действий сотрудников, пользующихся социальными сетями в рабочее время. В настоящее время риски значительно возрастают, так как любая информация о людях со всего мира, зарегистрированных в социальных сетях, связана с их профессиональными данными через глобальные «облака» информация. Кибер-преступники знают об этом и используют любые уязвимости в системе для получения прибыли. (Источник: http://belpak.mogilev.by директор по исследованиям компании Norman ASA на конференции Virus Bulletin)
- любой пользователь может создать фальшивую страницу от имени компании, с которой он никак не связан. Другими словами, он не только вводит в замешательство огромное количество пользователей, но и тем самым наносит значительный вред репутации данной компании.

53 - зараженность компьютеров

- По исследованию компаниий Panda Security, посвященному определению индекса риска соцсетей для предприятий, работающих в отраслях малого и среднего бизнеса, наиболее уязвимыми оказались такие популярные ресурсы как Facebook, Twitter и YouTube. Так, сеть Facebook заняла первое место по заражениям вредоносным ПО и нарушениям конфиденциальности, а также финансовых потерь вследствие утечки важной информации (19).
- Что касается безопасности, риск размещения информации о компании в социальных сетях обусловлен, прежде всего, уязвимостью популярных в Интернете платформ, вследствие чего возникает вероятность кражи личных данных и заражения. На социальных сетях вполне можно подхватить вирус, а логины или пароли могут быть украдены неизвестным лицом, которое в дальнейшем может полностью управлять корпоративной страницей компании.

54 **5. Использование социальных сетей в военных и политических целях**

55 Социальные сети вскоре после начала роста их популярности стали использоваться для шпионажа и дезинформации военными, для информационных войн и дестабилизации в политических целях (4).

56 А) Слежка за инакомыслящими через социальные сети активно используется госбезопасностью большинства стран, о чем периодически просачивается информация в масс-медиа

57 Б) Ведение кибервойн через соцсети

58 В октябре 2011 г. начальник стратегического командования армии США генерал Роберт Келер прямо заявил о том, что пора заняться разработкой концепции ведения наступательных кибероперацій, целью которых становились бы компьютерные (технические) и социальные сети. Генерал посетовал, что в этом году американская военная машина

столкнулась с проблемой необходимости проведения кибератаки против войск Муаммара Каддафи, но не была к этому готова. В 2008 г. западные спецслужбы развязали информационную войну против России в связи с агрессией в Южной Осетии, в т.ч. и в социальных сетях. Однако, через те же социальные сети пошла контринформация о действиях грузинских военных в Осетии от людей, которые сами или их родственники оказались в районе боевых действий. (Источнк: www.securitylab.ru)

59 В) Поиск преступников

60 Впервые в России, в Тамбовской области возбуждено уголовное дело в отношении 16-летнего учащегося колледжа, который допустил в социальной сети оскорбительные высказывания в адрес полицейского. Дело возбуждено по 319-й статье УК РФ («оскорбление представителя власти»). (13.10.11 - сайт Следственного комитета РФ). На сайте «Одноклассников» опознали по фото молодых преступников, похитивших пневматические пистолеты в магазине. При просмотре фотоальбомов в сети была обнаружена фотография, на которой два друга позируют с украденными пистолетами.

61 Г) Подготовка революций и митингов протеста

62 Яркими примерами могут служить весенние революции на Ближнем Востоке, движение «Революция через социальную сеть» в Белоруссии (название серии гражданских акций протеста, вызванных недовольством части населения действиями руководства страны, приведшими к финансовому кризису, девальвации белорусского рубля и резкому скачку цен - http://www.newsru.com/world/15jun2011). Акции протеста организовываются инициативными группами через социальные сети ВКонтакте и Facebook), подготовка митингов протестов против фальсификации выборов 4.12.11 в России и т.п..

63 **6. Зависимость от социальных сетей**

64 Еще в 2008 г. на конгрессе в Королевском колледже психиатров Великобритании этот вид Интернет-зависимости был признан психиатрами более серьезным явлением, чем зависимость от компьютерных игр (20).

65 Проводя исследования о влиянии социальных сетей на человека, российские ученые обнаружили, что такие популярные сайты, как «Одноклассники» и «В Контакте», стали для людей зависимостью, как и игры в Интернете. Они подсчитали, что, при ежедневном заходе в социальную сеть, пользователь тратит времени больше, чем на игры. Минимальные затраты на режим он-лайн для социальных сетей в среднем составляют около 3 часов в сутки. Максимум времени пребывания онлайн - 30 часами беспрерывного пребывания в социальной сети (9,13,20).

66 Недавно в Великобритании было проведено исследование влияния социальных сетей на здоровье человека. По данным исследования, социальные сети негативно влияют на работу иммунной системы организма, гормональный баланс, работу артерий и процессы мышления. У пользователей социальных сетей зачастую развивается слабоумие (исследователи из Германии, Японии,США) (13).

67 Такую высокую зависимость ученые объясняют, в первую очередь, человеческой потребностью к общению. Однако, психологи утверждают, что общение в социальных сетях не способствуют установлению контактов между людьми. Интернет-общение – это иллюзия и подмена реальной жизни. Люди в буквальном смысле слова становятся батарейками в матрице, и подпитывают виртуальную реальность, теряя собственные силы и здоровье, разрушая себя и окружающих. В мире «Одноклассников» все просто и легко, в социальных сетях не нужно решать социальных проблем – если человек тебе не нравится, его можно

«уничтожить» одним кликом, и подобрать себе другого виртуального друга, с подходящими параметрами.

68 **Выводы**

69 Социальные сети расширили кругозор современного человека, упростили общение, дали новое направление развитию глобальной Интернет-среды. Однако, пользование социальными сетями требует следования таким же правилам техники безопасности как пользование автомобилем или горючими материалами. Любой пользователь социальной сети должен помнить, что он может пострадать от того или иного вида риска, поэтому наибольшую важность приобретает выработка:

70 а) индивидуальных мер защиты своего профиля в сети, особенно ознакомления детей и подростков, с правилами безопасности при работе с социальной сетью,

71 б) необходимых мер, которые должны предпринимать владельцы сетей, для усиления безопасности своих пользователей,

72 в) работодателей, использующих сети в профессиональном плане для того, чтобы обезопасить свою компанию от возможного ущерба,

73 г) проработка вопросов, связанных с безопасностью в социальных сетях на государственном уровне.

74 Мы не перестаем пользоваться газовой плитой только потому, что существует вероятность устроить взрыв. Мы просто соблюдаем правила безопасности и не подпускаем к плите маленьких детей. Точно так же надо относиться и к социальным сетям.

Риски пользования социальными сетями

Бобкова И. А.
ГАУГН, доцент
Российская Федерация, Москва,

Аннотация

Социальные сети на данном этапе - самый динамично развивающийся сектор Интернета. Каждый год количество пользователей социальных сетей увеличивается на десятки миллионов человек. Самую популярную мировую сеть Facebook посещает более 700 млн. пользователей в месяц. Но только в последние годы аналитики, пользователи и владельцы социальных сетей стали всерьез задумываться о рисках и опасностях этого сектора Интернета

Ключевые слова: социальные сети, использование социальных сетей, риски пользования социальными сетями

Дата публикации: 30.11.2012

Ссылка для цитирования:

Бобкова И. А. Риски пользования социальными сетями // Искусственные общества. 2012. Т. 7. Выпуск 1-4 [Электронный ресурс]. Доступ для зарегистрированных пользователей. URL: https://artsoc.jes.su/s207751800000046-9-1/ (дата обращения: 23.09.2020).
