Содержание

Введение

Многие из нас думают и размышляют о будущем – каким оно будет? Мы с интересом читаем прогнозы ученых и часто убеждаемся в том, что они очень далеки от истины. Десять лет назад никто не придавал значения новому тогда явлению – социальным сетям и сайтам, предназначенным для общения.

И вот часть будущего мира создается на наших глазах – почти каждый из нас участвует в той или иной социальной сети, проводя там время, общаясь, находя друзей и темы для общения и творчества. И социальная сеть очень быстро меняется и реагирует на наши действия, как зеркало, в котором мы видим себя со своими достоинствами и недостатками, проблемами и достижениями.

Будущее будет таким, какими мы захотим его сделать, мы в будущем станем такими, какими хотим стать сейчас и это точно показывают нам социальные сети.

Историческими предпосылками возникновения социальных сетей стали гостевые книги (web-приложения, состоящие из списка сообщений, показанных от последних к первым, которые может оставить каждый посетитель)[1], форумы (сообщения группируются тематически, каждый посетитель может оставить сообщение на заданную тему в ответ на предыдущее) и блоги - каждый участник ведет журнал, аналогичный личному дневнику, его сообщения сортируются в хронологическом порядке, а другие посетители могут оставлять комментарии к сообщениям, при этом пользователь может создавать списки «друзей» или ограничить доступ к своему журналу.

Постепенно на базе этих форм интернет-общения начали образовываться социальные сети, отличительной чертой которых является наличие явно установленных связей между участниками.

Все социальные сети имеют ряд общих свойств: наличие регистрации (так называемой учетной записи) пользователя, при регистрации пользователь

[1] http://klasnaocinka.com.ua/ru/article/chto-takoe-sotsialnie-seti-istoriya-sozdaniya-sots-2.html

указывает некоторую информацию о себе, по которой его можно идентифицировать. Далее, вход в соцсеть происходит путем открытия сеанса, при этом пользователь указывает имя и подтверждает свою личность вводом пароля, кроме того, производится настройка свойств общения в соцсети, например, указание дополнительных данных о себе, своих интересов.

По мнению современных социологов, социальные сети – основная причина, по которой сегодня растет количество времени, проводимого в Интернете.

Главные преимущества социальных сетей – возможность пользователей заявлять о своих интересах, и разделять их с окружающими. И это дает основания утверждать, что социальные сети являются не только средством для общения, но и мощным маркетинговым инструментом, более того, исследователи полагают, что вскоре они станут необходимым инструментом для ведения производственной деятельности. Социальные сети служат площадкой для неформального общения, помогают создавать новую музыку и произведения искусства, служат серьезным инструментом для поиска сотрудников, единомышленников и партнеров.

С технической точки зрения, социальная сеть — интерактивный многопользовательский web-сайт, содержание, или, как принято говорить, контент которого наполняется самими участниками сети.

Совершим небольшой экскурс в историю. Многие исследователи полагают, что зарождение социальных сетей началось практически с рождения самого интернета в 1969 году[2]. На протяжении всей эволюции соцсетей можно выделить два основных направления развития: сугубо профессиональные сообщества и неспециализированные сети. Производными от профессиональных сообществ являются сети, объединяющие людей одними интересами или хобби.

[2] http://vsetke.ru/post/20447276

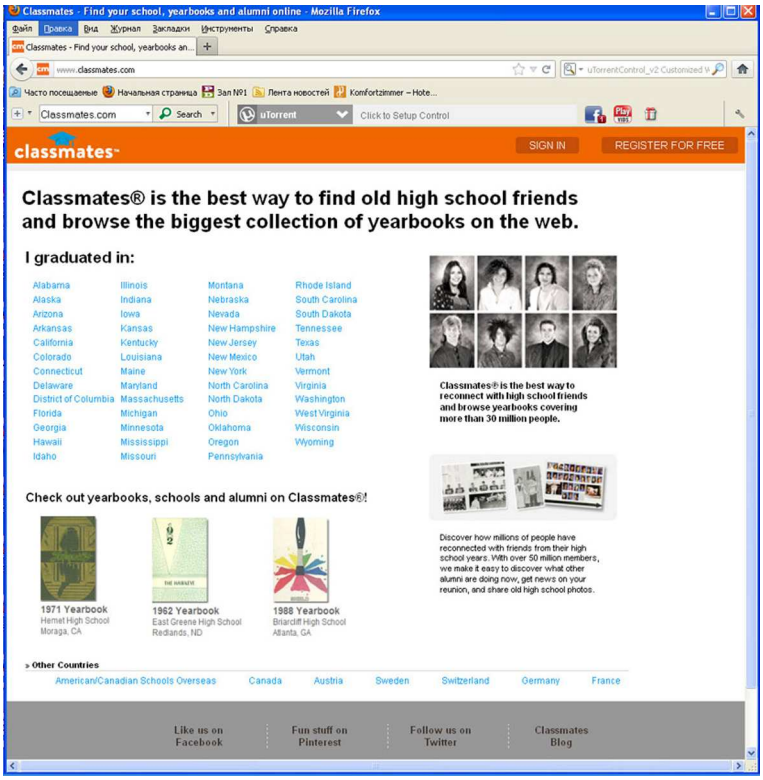

Рис.1. Первый сайт одноклассников

Итак, будем считать самым первым социально-сетевым ресурсом сеть Classmates.com, созданную Рэнди Конрадсом в 1995 году (рис.1). Classmates и переводится как «одноклассники». Сайт предоставлял пользователям возможность восстановить связь с бывшими одноклассниками, однокурсниками, сослуживцами, друзьями. Сеть действует по сей день и насчитывает больше 50 млн. пользователей в США и Канаде. Кроме того, её услуги доступны жителям Швеции, Германии, Австрии и Франции. Но довольно долгое время этот портал не поддерживал функции создания личных профилей и добавления друзей. То есть, пользователя могли соединить только с его учебным заведением и предоставить ему список обучавшихся в этом заведении.

Рис.2. Сайт, основанный на теории 6 рукопожатий

Именно поэтому некоторые исследователи считают первой полноценной социальной сетью не Classmates, а проект SixDegrees.com (рис.2), запущенный в 1997 году. В то время многие веб-сервисы (сайты знакомств, например) предлагали такие функции, как создание личной страницы или списка друзей, но по отдельности. SixDegrees.com стал первым социально-сетевым сервисом, который объединил эти функции, а в 1998 году добавил поиск по страницам друзей. Этот проект был наиболее приближен к современным соцсетям, однако, в 2001 году портал SixDegrees.com прекратил свое существование. Основатель сети Эндрю Вейнрейх объяснил это тем, что сервис просто опередил свое время. Ведь в 2000 году доступ к Интернету имели меньше половины жителей США. Иначе говоря, у зарегистрированных пользователей не было достаточного количества друзей и знакомых с доступом к интернету, чтобы общение на этом сайте было хотя бы интересным.

С 1997 г. по 2001 г. наблюдается первая волна социальных сетей. Затрону только самые известные из них.

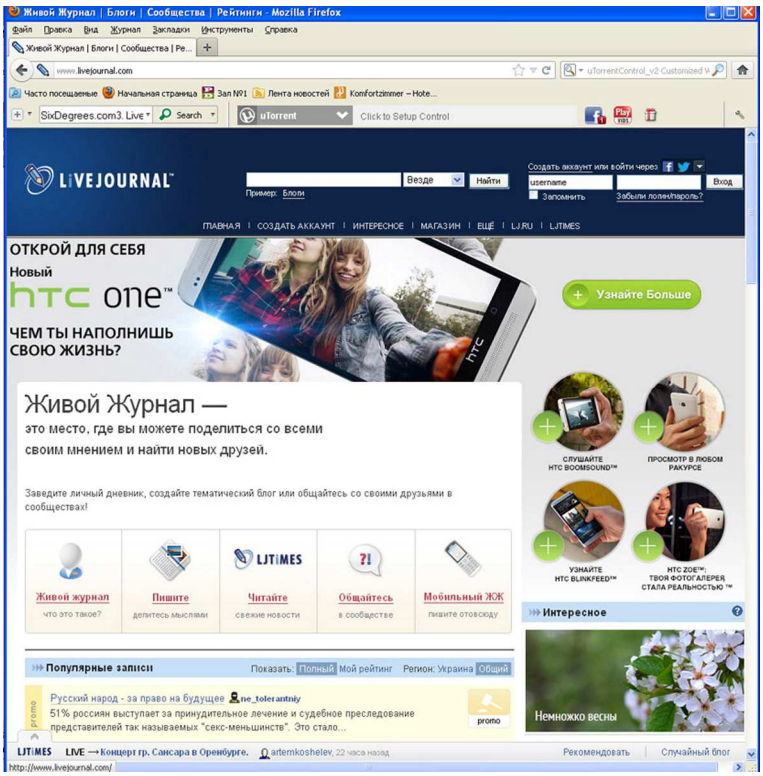

Рис.3. Первый блогохостинг

В 1999 году американским студентом-программистом был открыт сервис Livejournal.com. Там можно было создать довольно детальный профиль. Вскоре сервис предоставил возможность добавлять контакты (друзей). Livejournal стал первым массовым хостингом блогов (электронных дневников) и первым западным социальным сервисом, ставшим популярным в России. По количеству российские пользователи стоят на втором месте после американских. Видимо поэтому, в 2007 году российская компания SUP полностью выкупила сервис у компании SixApart.

В 2000 году появился шведский LunarStorm, в 2001 – корейский Cyworld.

Рис.4. Сеть для бизнесменов

Вторая волна распространения соцсетей пришлась на 2001-2004 годы. Для социальных сервисов, появившихся в этом промежутке времени характерно разделение по нишам, одной из которых стал бизнес. Первым веб-ресурсом, ориентированным на инициирование и поддержание деловых контактов, стал в 2001 году Ryze.com (рис.4). Этот проект дал толчок к формированию таких известных веб-сервисов, как LinkedIn и Friendster. LinkedIn стал мощным сетевым ресурсом в этом направлении. Friendster переоценил свои возможности и попросту не вынес наплыва посетителей. Постоянные технические трудности на сервисе привели к тому, что часть пользователей ушли на другие сайты, в частности на MySpace.

В 2003 году была создана сеть MySpace (рис. 5), основными пользователями которой стали рок-коллективы. Для независимых музыкантов портал стал своеобразной площадкой для самопрезентации. Кроме того, у поклонников рок-музыки появилась возможность общаться со своими кумирами и даже добавлять их в друзья. На сегодняшний день MySpace вторая по величине социальная сеть после Facebook.

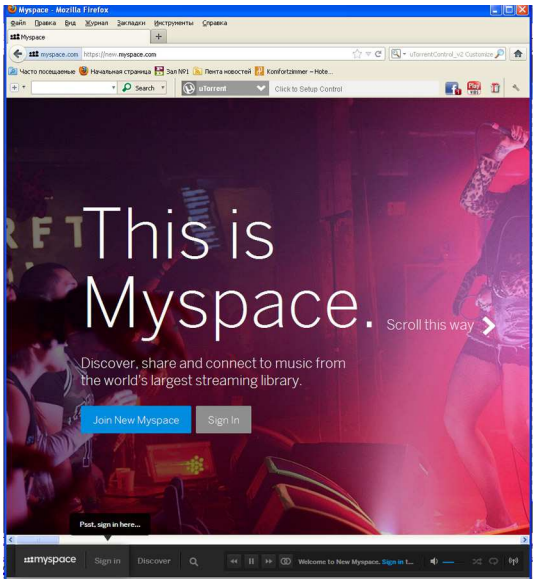

Рис.5. – MySpace -Музыкальное направление соцсетей

С 2004 года всевозможные интернет-сообщества из самых различных ниш стали использовать на своих сервисах инструменты соцсетей. В России к ним относятся MoiKrug.ru и Professionali.ru. На общих интересах основываются такие сети, как Dogster.ru – для владельцев собак, Couchsurfing.com – для путешественников, Care2.com – для активистов и волонтеров, MyChurch.com – для приверженцев христианских конфессий.

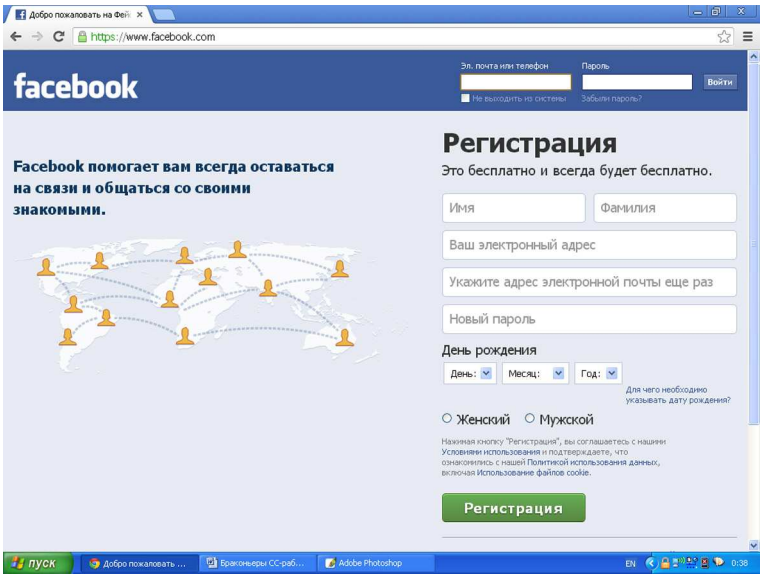

Рис. 6. FaceBook - один из лидеров соцсетей

В 2004 году Марком Цукербергом, студентом из Гарварда, был запущен портал Facebook (рис.6), который сегодня является крупнейшей социальной сетью. Но изначально регистрация была доступна лишь гарвардским студентам. Постепенно к Facebook получили доступ студенты других ВУЗов, а потом

учащиеся колледжей и школьники. К 2008 году Facebook отобрал у MySpace пальму первенства и стал крупнейшей в мире соцсетью, сервис которой доступен на 40 языках.

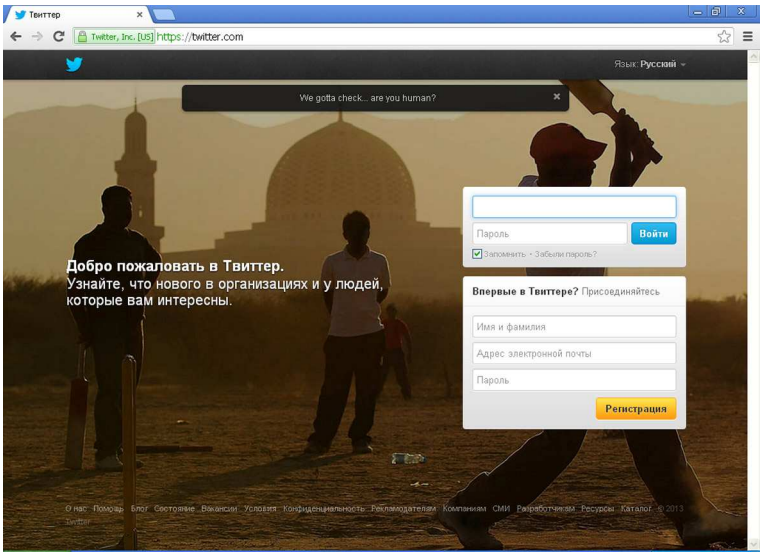

Рис. 7. Twitter - зафоловимся?

Американский программист Джек Дорси запустил в 2006 г. проект Twitter (рис 7), который наиболее динамично развивался среди новых социально-сетевых проектов. Сервис сравнивают с обычным блогохостингом, но специфика работы с ним, форма сервиса, а также стиль сообщений несколько иные, нежели в блогах. В 2008 г. во время теракта в Мумбаи Twitter стал свидетельством того, что эволюция соцсетей обусловила появление новых путей информирования в СМИ.

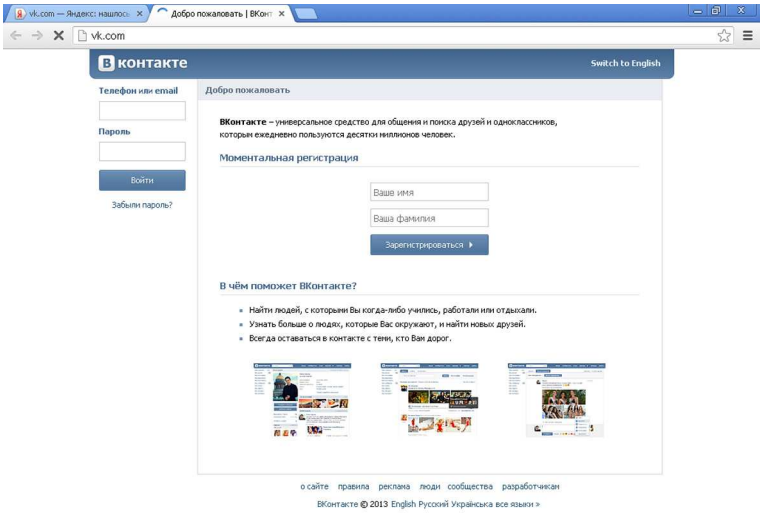

Рис. 8 – Вконтакте - лидер в СНГ

Совершая путешествие во времени, мы добрались и до российских проектов соцсетей. Проект «В контакте» основал в 2006 г. петербургский программист Павел Дуров (соавтор – его брат Николай). Во многом сайт копирует популярный Facebook, хотя авторы проекта это опровергают. Сегодня сеть «В контакте» является самым крупным в СНГ социально-сетевым ресурсом. Он входит в 30-ку самых посещаемых порталов мира. Кроме того, «В контакте» известен, как самый крупный видео- и аудиохостинг в рунете.

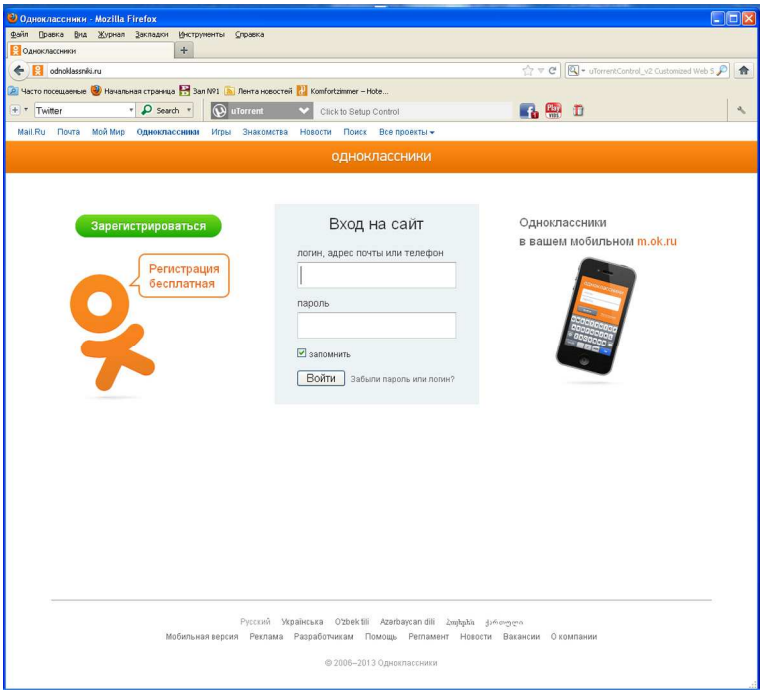

Рис. 9. Одноклассники - они и в Африке одноклассники

В том же 2006 г. появился на свет российский аналог сети Classmates.com – «Одноклассники», автором которого является Альберт Попков. Социальная сеть используется для общения с бывшими и настоящими одноклассниками, однокурсниками и просто друзьями. По последним данным, которые пресс-служба «Одноклассников» предоставила Вестям.ру, в соцсети насчитывается больше 67 млн. зарегистрированных пользователей. Для сравнения, социальная сеть «В контакте» (главный конкурент «Одноклассников») насчитывает более 100 млн. участников.

Приведем краткий перечень социальных ресурсов в таблице.

Название сайта	**Адрес в сети**
Best Persons – Лучшие люди.	bestpersons.ru

(www.bestpersons.ru)	
Одноклассники – самая посещаемая социальная сеть Рунета	odnoklassniki.ru m.odnoklassniki.ru
Одноклассники на KM.RU	odnoclassniki.km.ru
ВКонтакте.ру – универсальное средство поиска знакомых	Vkontakte.ru Vk.com m.vkontkte.ru
В комнате – место, где можно увидеть друг друга. Бизнес, общение, интерактив	vkomnate.com
Мир тесен!	mirtesen.ru
Мой мир@Mail.Ru – сообщество пользователей почтового сервиса Mail.ru	my.Mail.Ru
Соседи-Онлайн.Ру – узнай все о своем районе и поделись с соседями на этом сайте.	sosedi-online.ru
Ваши соседи – сайт знакомств между соседями, живущими в мегаполисах, для общения в реальной жизни	vashisosedi.ru
Memori.ru – («социальные закладки») возможность размещать ссылки с небольшими комментариями	memori.ru
МОЯ ШКОЛА – общероссийский образовательный портал – образование, новости	1class.ru
Мой круг	moikrug.ru
Сайт знакомств «Ваш блокнотик»	love.bloknotik.ru
Dating.ru – знакомства, общение, чаты, сайт знакомств	Dating.ru
iFlirt.RU – Романтические знакомства	Iflirt.ru
Привет.ру – – Сайт о людях и интересах. Общение, блоги, сообщества, фото, видео.	www.privet.ru

Найди новых друзей	
Тумбала - социальная сеть нового поколения	Tumbala.com
Путь к другим – интеллектуальный сервис знакомств и общения.	putj.ru

И конце нашего небольшого введения немного стихотворного юмора на тему социальных сетей:

Крошка-сын к отцу пришел
И спросил с тоскою: "Одноклассники", отец –
Это что такое?
Это что за сайт такой, где седые люди,
На реал махнув рукой, утопают в блуде?

Где к изменам виден путь, цель ясна и средства,
Где хотят себя вернуть в брежневское детство?
Там нарушен их покой! Там проводят ночи!
Это что ж за сайт такой? - объясни мне, отче?

И тогда сынку сказал папочка сказал спокойно:
База данных ФСБ - вот что мы такое!

Ну и что? – сказал сынок, - ради старой дружбы
Хоть какой-то будет прок людям от спецслужбы!
Сколько найдено друзей, вспомнено моментов
Столько на планете всей не найти агентов.

Чтоб в недетскую игру заманить всех сразу,
Еще сайт "вконтакте.ру" пополняет базу.
Все вы правильно поймете, если нет, то знайте:
У нас все те на учете, кого НЕТ на сайте!

Основой, ядром каждой главы этой книги является СОВЕТ - короткая рекомендация, что нужно делать в том или ином случае нашей виртуальной жизни в соцсети. В главе также могут быть части - ЭТО ИНТЕРЕСНО и ДЛЯ ОПЫТНЫХ ПОЛЬЗОВАТЕЛЕЙ.

1. Ваш компьютер – оборотень

Вы уверены, что через ваш личный гаджет за вами никто не следит? Соцсеть приходит прямо к вам на домашний компьютер, поэтому защитите его. В нём без особого труда можно поселить программу доступа к данным и скачивания файлов.

Невиданные прежде «информационные катастрофы», аналогичные публикации сотен тысяч критичных для политики и бизнеса документов в WikiLeaks[3], дают представление о том, какие чудовищные объемы данных могут быть похищены с использованием современных технологий и к каким последствиям это может привести. Еще совсем недавно событий сравнимого масштаба не могло быть в силу существовавших технических ограничений на объемы данных, которые могли попасть в руки злоумышленников, — просто не было носителей и скоростей передачи данных, позволяющих украсть, например, полный комплект документации на изделие под названием "нейтронная бомба". Теперь необходимый объем данных уложится на нескольких квадратных миллиметрах флэш-памяти, да и хранятся они в цифровой форме, как будто специально созданной для упрощения краж. В итоге угроза кражи данных (data theft) и несанкционированный доступ к данным (data breach) вошли сегодня в число критичных.

Угрозы безопасности становятся все разнообразнее, так например Секретная служба США, которая в отличие от своего российского аналога, Федеральной службы охраны РФ, помимо своей непосредственной функции выпускает общедоступные отчеты, где представляет существующие и новые угрозы национальной безопасности. Последний из них 2010, Data Breach Iinvestigations Report, посвящен всестороннему анализу статистики хищений данных и аккумулирует данные о компьютерных атаках, публикуемые в странах Северной Америки и Западной Европы, Китае, Египте и Японии. Остальные страны, в том числе и Россия, не предоставляют таких официальных

данных. Половина хищений фиксируется в США, где около 70% потерь данных приходится на три сектора экономики: финансовый (33%), гостиничный (23%) и торговлю (15%). Документ начинается с констатации факта наметившихся изменений в статистике компьютерных преступлений — хотя внешние хакерские атаки и проникновения все еще остаются основным способом хищений (на них приходится 70%, а на внутренние — 48%, сумма не равна 100%, поскольку часто злоумышленники действуют совместно), показательна динамика последнего года: внешние сократились на 9%, а внутренние увеличились на 26%.

Наш домашний компьютер, с помощью которого мы входим в Интернет, содержит данные – файлы, документы, фотографии и программы, которые с этими данными оперируют – показывают нам фотографии, дают возможность писать и сохранять тексты, вводить данные с клавиатуры и передавать текстовые сообщения, наш голос и изображение нашим друзьям в Интернете. Программы – это активная часть как нашего компьютера, так и компьютерной системы, в которую он включен. Именно с помощью программ мы делаем все необходимые нам действия, обрабатываем наши данные и именно от них получаем информацию, видим компьютерный мир их глазами.

Программы могут быть уже установлены на компьютере при его покупке – это операционная система и минимальный набор программ для работы с документами, фото и видео. Дополнительные программы могут быть добавлены нами самими, например, средства для общения в сети, игры, средства работы с нашим мобильным телефоном. Но программы могут появиться на нашем компьютере и без нашего ведома, например, записаться на наш компьютер при посещении различных сайтов. И все они могут обращаться с нашими данными или, как говорят специалисты в области информатики, иметь к ним ДОСТУП. Классификацию внедренных в наш компьютер программ мы дадим позже, но чаще всего их называют троянами или троянцами, по аналогии и ассоциации со знаменитым троянским конем. Попав

[3] http://www.osp.ru/os/2010/10/13006330/

на компьютер, эти вредоносные программы передают на другие компьютеры ваши данные и если к компьютеру в этот момент подключена флеш-память, мобильные телефон, электронная книга, то эти программы смогут прочитать и их.

Недавно эксперты сообщили об обнаружении новой модификации мобильного трояна Trojan-SMS.J2ME.Konov.b[4], массово распространяющегося в социальной сети «ВКонтакте». Эксперты отмечают также, что это новый этап эволюции распространения мобильного вредоносного программного обеспечения.

Троянская программа Trojan-SMS.J2ME.Konov хорошо известна экспертам, ее сигнатуры были добавлены в антивирусные базы еще в мае 2008 года. Новая версия отличается методом распространения: для доставки мобильного вредоносного ПО вирусописатели впервые задействовали социальную сеть.

Заражение данной троянской программой происходит по следующей схеме. Войдя на сайт, пользователь «ВКонтакте» получает сообщение от имени человека, внесенного в список друзей, с рассказом о возможности бесплатно пополнить свой мобильный счет. В сообщении предлагается через указанную ссылку скачать на мобильное устройство JAVA-программу, при подключении к которой якобы произойдет пополнение мобильного счета участника акции на сумму от 500 до 555 рублей.

На самом деле после установки указанного JAVA-приложения на мобильный телефон и его запуска, троянская программа отправляет SMS-сообщение на пять коротких премиум-номеров, списывая, таким образом, сумму за отправленные сообщения со счета зараженного телефона. Стоимость одного SMS-сообщения, отсылаемого троянцем с инфицированного телефона, составляет порядка 250 рублей. Префиксы сообщений и сами номера берутся из manifest-файла, хранящегося внутри jar-архива. В ряде случаев загрузка троянца сопровождается попыткой получить логин и пароль пользователя сайта

[4] http://www.softblog.info/security/mobilnyie-troyanyi-v-sotsialnyih-setyah/

«ВКонтакте» через подложный сайт с помощью фишинг-технологий (об этих технологиях читайте ниже). Получив такие данные, злоумышленники рассылают спам от имени обманутого пользователя через его контакт-лист.

В мае 2013 года компания «Доктор Веб» — российский производитель антивирусных средств защиты[5] — обнаружила неизвестный ранее функционал в новой вредоносной программе для Facebook, о которой сообщали многочисленные сетевые СМИ. **Trojan.Facebook.311** может не только публиковать от имени пользователя новые статусы, вступать в группы, оставлять комментарии, но и рассылать спам в социальных сетях Twitter и Google Plus.

Троянская программа **Trojan.Facebook.311** представляет собой написанные на языке JavaScript надстройки для популярных браузеров Google Chrome и Mozilla Firefox. Злоумышленники распространяют троянца с использованием методов социальной инженерии — вредоносные программы попадают в систему при помощи специального приложения-установщика, маскирующегося под «обновление безопасности для просмотра видео». Примечательно, что установщик имеет цифровую подпись компании Updates LTD, принадлежащей Comodo. Надстройки называются Chrome Service Pack и Mozilla Service Pack соответственно.

После завершения установки в момент запуска браузера **Trojan.Facebook.311** пытается загрузить с сервера злоумышленников файл с набором команд. Затем встроенные в браузеры вредоносные плагины (набор команд) ожидают момента, когда жертва выполнит авторизацию в социальной сети Facebook. После этого троянец может выполнять от имени пользователя различные действия, обусловленные содержащимися в конфигурационном файле командами злоумышленников: поставить «лайк», опубликовать статус, разместить на стене пользователя сообщение, вступить в группу, прокомментировать сообщение, пригласить пользователей из списка контактов жертвы в группу или отправить им сообщение. Помимо этого троянец может по

[5] http://news.drweb.com/show/?i=3527&lng=ru&c=14

команде злоумышленников периодически загружать и устанавливать новые версии плагинов, а также взаимодействовать с социальными сетями Twitter и Google Plus, в частности, рассылать спам.

Попробуем разобраться, что можно сделать для борьбы с «невидимыми наблюдателями» на нашем компьютере[6]?

Идея достаточно проста – необходимо сделать на компьютере несколько изолированных рабочих областей или, говоря языком опытных пользователей создать несколько учетных записей и профилей.

Например, дети хотят играть и общаться в сетях, а родителям кроме личного общения нужна еще и стабильная работа компьютера и сохранность своих данных. Поэтому возникает необходимость настроить домашний компьютер на работу нескольких пользователей.

Цель такой настройки: разделение доступа пользователей к файлам, папкам, программам.

Для демонстрации этого подхода пользователей разделим на родителей и детей.

В операционных системах (ОС) семейства Windows, начиная с Windows NT, есть понятие «учетная запись».

Учетная запись предназначена для идентификации пользователя (подробно об идентификации и аутентификации написано в разделе «Это интересно» данной главы) и определения его прав в ОС.

Когда пользователь один, то обычно при запуске ОС виден экран приветствия, а затем сразу появляется рабочий стол. Пользователь при этом имеет все права в ОС. В таком случае говорят, что пользователь вошел в операционную систему под встроенной учетной записью администратора.

Для настройки нескольких пользователей необходимо создать несколько учетных записей. Для этого необходимо запустить консоль «Управление компьютером».

[6] http://www.pc-user.ru/view_post.php?id=60

Также пользователей можно настраивать через утилиту «Учетные записи пользователей», которая запускается из Панели управления.

Запуск консоли выполняется следующим образом – необходимо щелкнуть правой кнопкой мыши по значку «Мой компьютер» и выбрать в появившемся меню пункт «Управление компьютером» или через «Пуск» - «Настройка» - «Панель управления» - «Администрирование» - «Управление компьютером».

Раскрываем в левом окне ветку «Локальные пользователи и группы» и выбираем папку «Пользователи».

Теперь в правом окне видны учетные записи пользователей ОС. По двойному клику по учетной записи открывается окно свойств.

На следующей картинке (рис. 1) показано окно свойств учетной записи «Гость».

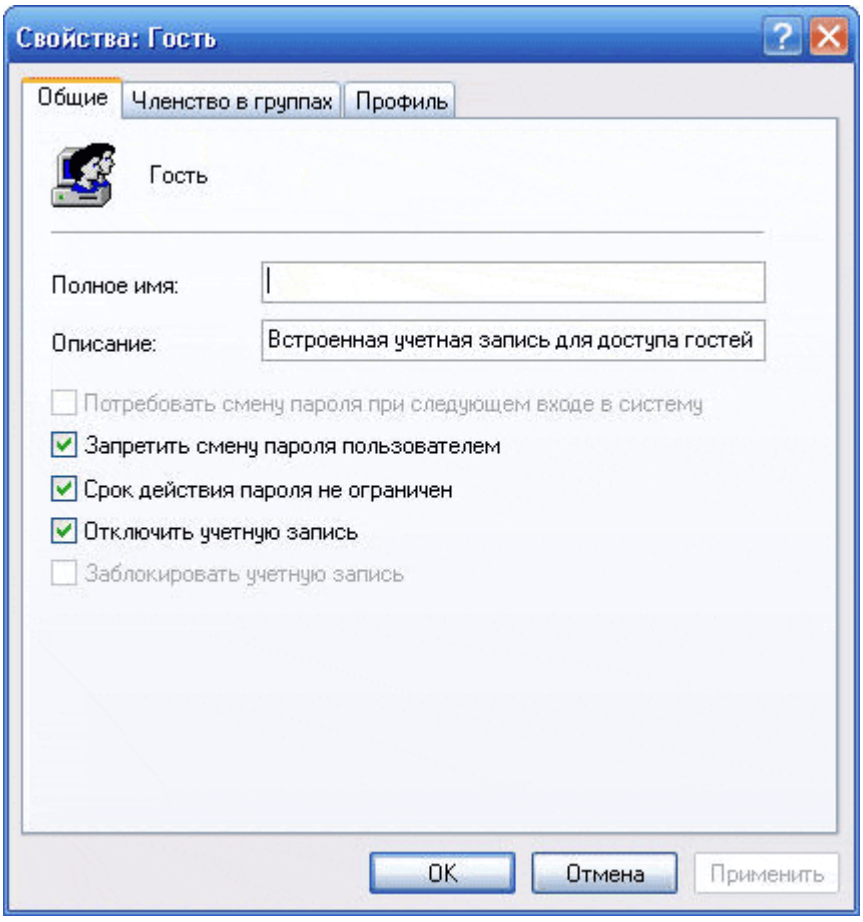

Рис. 1 Учетная запись «Гость»

Учетная запись «Гость» предназначена в основном для обеспечения минимального доступа к ресурсам компьютера по сети.

Запись «Admin» - это встроенная учетная запись администратора, обычно после установки ОС, пользователь загружается под ней. В зависимости от версии (сборки) ОС эта запись может также называться «Administrator» или «Администратор».

На закладке «Общие» можно указать полное имя и описание учетной записи, а также настроить некоторые свойства пароля учетной записи.

Рассмотрим назначение этих свойств.

Потребовать смену пользователя при следующем входе в систему.

Если эта галочка установлена, то при следующем входе в систему ОС попросит пользователя сменить пароль.

Это свойство предполагается применять следующим образом: системный администратор создает новую учетную запись с каким-нибудь стандартным простым паролем, например «12345». Затем пользователь при входе в ОС под этой новой учетной записью меняет пароль на свой собственный.

В результате должно получиться, что пароль пользователя знает только сам пользователь, при этом рекомендуется использовать пароль не меньше 6-8 символов, содержащий буквы в верхнем и нижнем регистре, цифры, спецсимволы.

Это свойство рассчитано на сознательных пользователей, например, пользователей группы «родители».

Запретить смену пароля пользователем.

Эта галочка при установке запрещает пользователю самостоятельно менять пароль. Эта свойство необходимо использовать, если пользователи не очень сознательные и хотят изменить сложный пароль, выданный системным администратором, на простой пароль.

Срок действия пароля не ограничен.

Если эта галочка не установлена, то пользователю периодически надо менять пароль. Если срок действия пароля истек, то запись блокируется.

Отключить учетную запись.

Эта галочка нужна при отключении учетной записи. Запись остается в ОС, но не работает. Это используется, например, когда пользователь уходит в отпуск, его запись отключается, и никто не сможет войти в ОС от имени этого пользователя, а после возвращения из отпуска снова включается.

Заблокировать учетную запись.

Эта галочка нужна для разблокирования записи. Пользователь ее может только убирать. Если учетная запись заблокирована по каким-либо причинам, то в этом поле появляется галочка, и для разблокирования записи ее надо снять.

Создание новой учетной записи.

Для этого надо в окне «Управление компьютером» выбрать ветку «Пользователи», затем в меню выбрать «Действие» - «Новый пользователь», как показано на рис. 2.

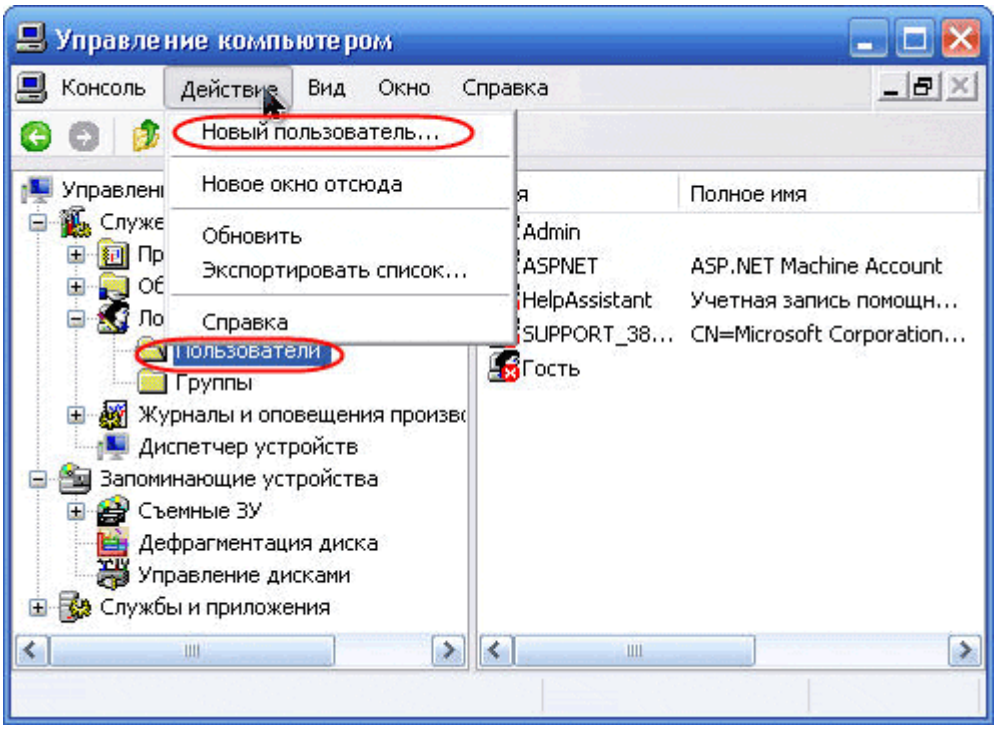

Рис. 2. Создание нового пользователя

Должно появиться окно создания новой учетной записи. В нем надо ввести имя пользователя, имя можно ввести даже кириллицей.

При желании можно ввести полное имя и описание, но эти поля больше используются в организациях, где много пользователей.

После имени надо 2 раза ввести пароль в поля «Пароль» и «Подтверждение».

Это сделано для того, чтобы не ошибиться при наборе пароля. Если пароль и его подтверждение не совпадают, то при создании появится сообщение об этом.

Из свойств пароля желательно не забыть снять галочку с «Потребовать смену пользователя при следующем входе в систему» и поставить «Срок действия пароля не ограничен».

В конце настроек нажать кнопку «Создать». После этого система создаст пользователя и предложит создать следующего. Если надо - создаем следующего пользователя, если не надо, то нажимаем кнопку «Закрыть».

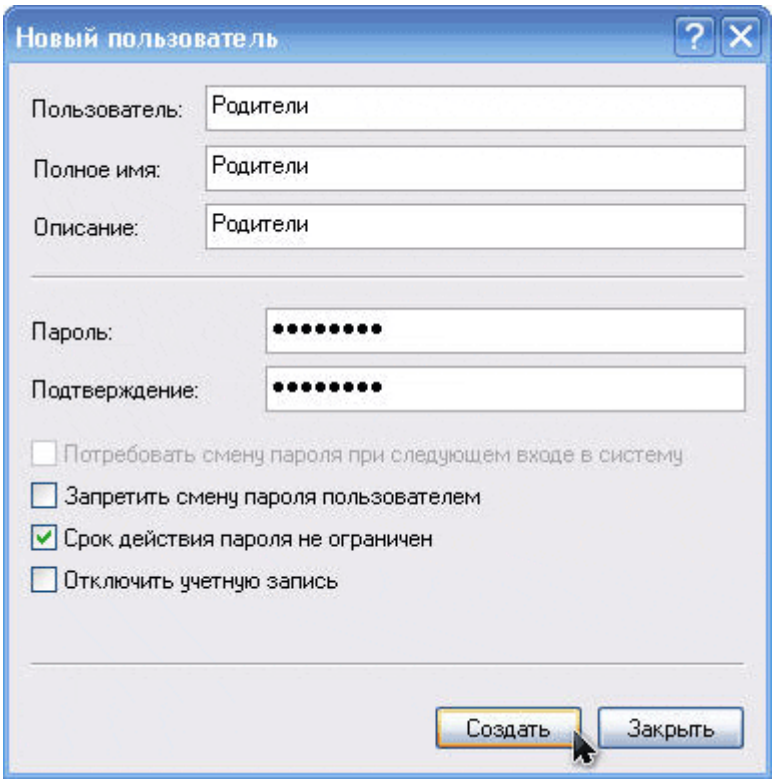

Рис. 3. Учетная запись для родителей

Таким образом создаем учетные записи для всех пользователей. В примере на рис. 3 создана запись «Родители».

На своем компьютере Вы можете создать пользователей на каждого члена семьи. Если пользователей будет несколько, то желательно на каждого создать свою учетную запись, а встроенную запись администратора ОС использовать только в случае возникновения проблем.

После этого надо создать или сменить пароль для текущей записи администратора.

Для этого выбираем в правом окне запись «Admin», затем в меню выбрать «Действие» - «Задать пароль».

При этом ОС выдаст предупреждения о последствиях такого действия.

Для начинающих пользователей надо согласиться и задать пароль. Пароль надо ввести два раза, чтобы избежать ошибок при его наборе.

Если в ОС не настроено (по умолчанию не настроено) ограничение на количество неудачных попыток, то пароль можно вводить бесконечное количество раз, а если настроено, то запись после определенного количества неудачных попыток блокируется.

Для начала я рекомендую попробовать создать простые пароли, например, «123456» всем пользователям и проверить их.

Для этого жмем «Пуск» - «Завершение сеанса» - «Смена пользователя».

После этого Вы должны увидеть примерно такую картинку (рис. 4):

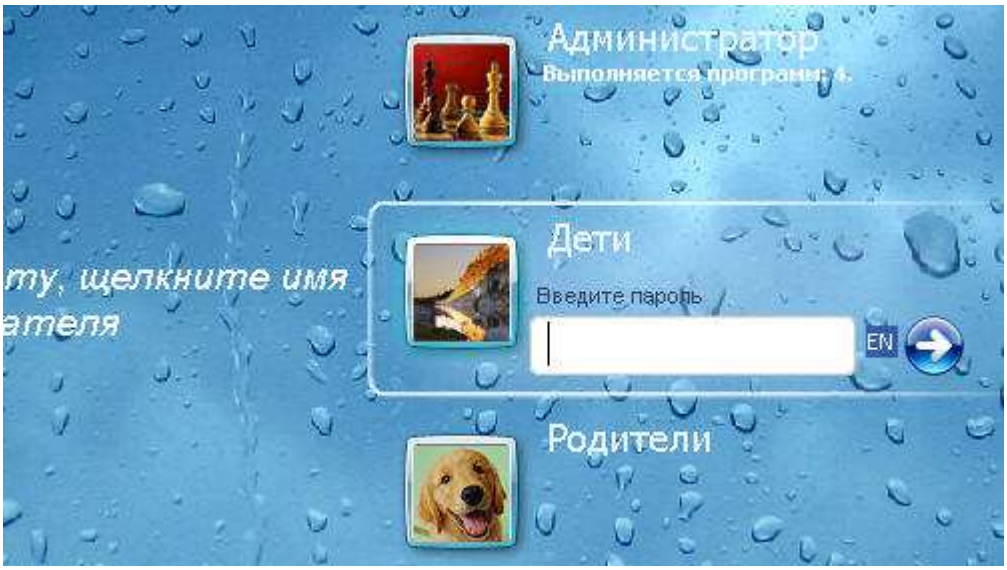

Рис. 4. Вход в операционную систему

В середине экрана есть подсказка «Чтобы начать работу, щелкните имя пользователя», слева внизу кнопка «Выключить компьютер».

На этом экране пользователю предлагается выбрать свою учетную запись (можно навести мышкой и нажать левой кнопкой мыши) и ввести пароль.

Если завершать предыдущий сеанс через «Пуск» - «Завершение сеанса» - «Смена пользователя», то программы предыдущего пользователя будут работать – это будет видно в строке под именем.

А если через «Пуск» - «Завершение сеанса» - «Выход», то все программы, запущенные пользователем, завершатся.

Системные программы ОС, а также программы, запущенные как системные, например, антивирус, продолжают работать при смене пользователей.

Это удобно использовать, когда надо быстро загрузить ОС под другим пользователем

Если вдруг при загрузке компьютера запись «Администратор» не будет видна, тогда нажмите комбинацию клавиш Alt+Ctrl+Del, должно появиться окно для ввода имени и пароля.

В нем надо набрать соответственно «Администратор» и правильный пароль, после чего эта запись загрузится.

Для проверки правильности выполненных действий попробуйте зайти под каждым пользователем, чтобы проверить правильность пароля и чтобы создались папки профилей пользователей на диске.

Папки профиля – это папки в «C:\Documents and Settings\» (рис.5).

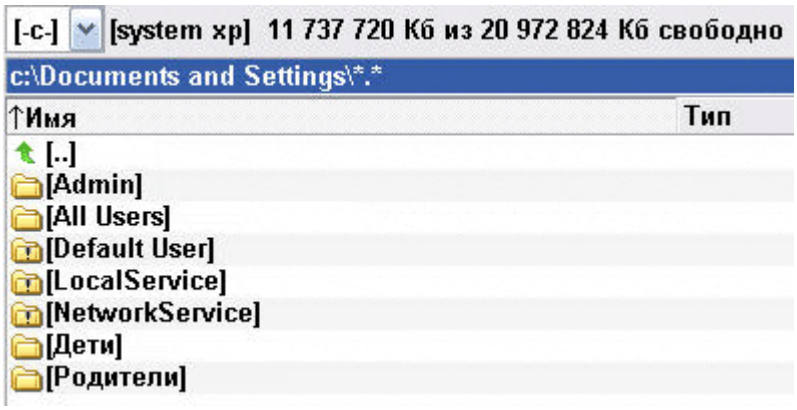

Рис.5. Папки профиля

После проверки простых паролей, попробуйте создать более сложные, какие Вам подойдут, и проверьте их.

Для всех пользователей надо создавать разные пароли.

После создания и загрузки новой учетной записи пользователь увидит на рабочем столе ярлыки программ, которые были установлены для всех пользователей.

Некоторые программы имеют возможность выбора при установке: «для всех пользователей» или «для текущего пользователя».

Настройки рабочего стола новых пользователей будут созданы «по умолчанию», но каждый пользователь может настроить его под свои нужды.

В рассматриваемой ОС все пользователи разделены по группам, в зависимости от того, какую работу они выполняют. В ОС уже есть встроенные группы, как показано на картинке ниже.

Пользователи ОС также могут создавать другие группы, если они являются членами группы администраторов ОС.

В случае домашнего компьютера новые группы создавать нет смыла, т.к. пользователей мало.

При создании новой учетной записи она попадает в группу «Пользователи». Этого достаточно для запуска программ, работы с документами, интернетом.

Для установки и настройки программ надо быть членом группы администраторов.

Изначально пользователи не имеют доступа к профилям других пользователей, при попытке доступа ОС выдаст сообщение об отказе в доступе.

Пользователя «Родители» надо добавить в группу администраторов.

Для этого устанавливаете курсор на группу «Администраторы», делаете двойной клик, появится окно «Свойства: Администраторы».

Слева внизу есть кнопка «Добавить», надо нажать ее.

После этого появится окно «Выбор: Пользователи».

В нем надо нажать кнопку «Дополнительно» слева внизу.

Появится окно поиска пользователей.

В нем надо нажать кнопку «Поиск». Затем в списке найти учетную запись «Родители», выбрать ее и нажать «ОК».

В окне «Выбор: Пользователи» появится строка такого вида:

«слово\Родители».

Первая часть (слово)– это имя компьютера, вторая – имя записи.

После этого надо нажать «ОК».

Пользователь «Родители» получает права администратора в ОС.

Нажимаем «ОК» и получаем, что пользователь «Родители» может просматривать профиль пользователя «Дети», а не наоборот. Все это может пригодиться также при чтении главы «Дети и сети».

В результате пользователь «Дети» не может без использования специальных системных методов и программ изменить файлы в профиле пользователя «Родители».

Если надо установить новые программы или игры или удалить старые, это можно сделать от пользователя «Admin» или «Родители».

Если программа или игра после установки не создаст ярлыки и/или группы ярлыков для пользователя «Дети», тогда надо ярлык запуска этой программы поместить в папку «C:\Documents and Settings\Дети\Рабочий стол\», пользователь «Дети» увидит этот ярлык на своем рабочем столе.

Совет: Создайте себе отдельную учетную запись (не с правами администратора) для работы в Интернет и общения в соцсетях, создайте другие учетные записи для членов семьи или ваших подчиненных на работе (также желательно не с правами администратора), установите на компьютер средства антивирусной защиты. По окончании сеанса общения всегда выходите из социальных сетей, чтобы посторонние пользователи или программы не могли выполнить действия от вашего имени.

ЭТО ИНТЕРЕСНО

В современной информатике компьютер чаще всего рассматривается в виде совокупности элементов, которые можно разделить на субъекты и объекты[7].

[7] Биктимиров М.Р., Щербаков А.Ю. Избранные главы компьютерной безопасности. – Казань: Изд-во казанского матем. общества, 2004. – 372 с.

Данное разделение основано на свойстве элемента компьютерной системы «быть активным» или «получать управление» (в компьютерной литературе применяются также термины «использовать ресурсы» или «пользоваться вычислительной мощностью»). Оно исторически сложилось на основе модели вычислительной системы, принадлежащей фон Нейману, согласно которой последовательность исполняемых инструкций для вычисляющего процессора (программа, рассматриваемая как «субъект» компьютерной системы) находится в единой среде с данными (выступающими в качестве «объекта»).

Здесь необходимо сделать важное уточнение. Обычно под субъектами имеются в виду люди, а под объектами – организации, технологические процессы, материальные продукты и услуги, то **в данном случае мы понимаем под субъектом программу, управляемую человеком, а под объектом – данные, обрабатываемые или порождаемые этой программой**.

Самое главное свойство нашего компьютера состоит в том, что пользователь воспринимает объекты и получает информацию только через субъекты, которыми он управляет и которые отображают информацию, относящуюся к окружающему миру. Иными словами - мы видим компьютерный мир, его ресурсы, других обитателей сети не своими глазами, а глазами своего компьютера, а еще точнее - глазами множества программ, которые на нем установлены и о большинстве которых обычный пользователь не имеет ни малейшего понятия.

На практике пользователь сообщает компьютеру свои запросы, используя такие инструменты управления, как клавиатура, «мышь», джойстик, сенсорный экран, электронное перо, которые являются внешним оборудованием компьютера и передают информацию субъектам нижнего уровня, обслуживающим эти устройства и также передающим информацию далее, субъектам или программным модулям операционной системы, обеспечивающим функционирование компьютера в целом. Отличие терминов «программа» и «программный модуль» состоит в том, что программа является

явлением более высокого порядка, чем программный модуль, а программный модуль является подсистемой, обладающей в рамках программы особой целостностью.

Из этого следует, что программа состоит из взаимосвязанной совокупности программных модулей. **Программа предназначена для решения законченной задачи, которая сформулирована ее разработчиком. Модули же решают отдельные подзадачи.** Например, программа текстового редактора Microsoft Word, предназначенного для работы с текстами и электронными документами, состоит из нескольких десятков программных модулей, часть которых относится к операционной среде Windows. Выделение программного модуля оправдано при решении задач управления доступом, о которых будет сказано ниже, а также при разработке программ для решения частных задач системных аналитиков.

Субъекты бывают разного уровня: нижнего – драйверы, обслуживающие внешние устройства компьютера, среднего – программы-субъекты операционной системы, обеспечивающие работу компьютера и пользователя независимо от решаемых ими задач, и верхнего – прикладные программы, обеспечивающие выполнение целевых функций.

Передача информации от субъектов верхнего уровня также происходит иерархически, только направление передачи информации меняется. Прикладные программы передают результаты своей деятельности операционной среде. Она, в свою очередь, передает информацию драйверам средств отображения, выводящим информацию на экран или другие средства визуального или графического отображения. Например, команда пользователя в меню программы текстового редактора «Сохранить файл» приводит к тому, что набранный в редакторе текст передается модулям операционной системы, последовательно передающим его модулям, управляющим работой жестких дисков или флеш-носителей. И только после этого на диске возникает файл, содержащий набранный текст. **Передача информации от одного объекта к**

другому происходит по инициативе субъекта, а сама такая передача называется «потоком» или «потоком данных».

Изменение и порождение новых объектов компьютерной системы производится субъектом, как активной компонентой, опосредованно управляемой пользователем. Именно субъекты порождают потоки информации и изменяют состояние объектов. Субъекты также могут влиять друг на друга через изменяемые ими объекты.

Пользователь – лицо (физическое лицо), аутентифицируемое некоторой информацией и управляющее субъектом компьютерной системы через органы управления компьютером. Пользователь КС является, таким образом, внешним фактором, управляющим состоянием субъектов. Аутентифицируемость пользователя означает, что он должен некоторым образом «представить себя» управляемой им КС, в противном случае компьютерная система не различит одного пользователя от другого. Представление пользователя компьютерной системе протекает обычно в два этапа: первый этап – идентификация – пользователь указывает свое имя, второй – собственно аутентификация – пользователь подтверждает свою индивидуальность некоторой никому не известной информацией, обычно паролем. Именно так мы представляемся в любой социальой сети. Процедуры идентификации и аутентификации есть своего рода «основа» компьютерной системы, поскольку без точного определения пользователей, без фильтра «свой-чужой» невозможно определение прав и функций пользователя в системе, его правильное позиционирование.

ДЛЯ ОПЫТНЫХ ПОЛЬЗОВАТЕЛЕЙ

Как полностью изолироваться от Интернет при помощи виртуализации и виртуальных машин?

Виртуальная машина – это специальная программа, которая создает «компьютер внутри компьютера».

Пользователь имеет возможность настроить несколько ОС (виртуальных машин) для работы.

Такой способ требует достаточно мощного компьютера, т.к. виртуальные машины используют действительные ресурсы – процессор, память, жесткий диск; пользователь получает одновременно две и более одновременно работающих ОС.

Файлы виртуальной машины на действительной ОС представляют собой один файл, и без запуска виртуальной машины доступ к ним получить нельзя.

Для этого в первую очередь необходимы две виртуальные операционные системы.

1. Установить VMware Workstation.
2. Создать необходимый образ операционной системы.
3. В операционной системе, имеющей выход в сеть, настроить виртуальный сетевой адаптер. VM->Settings->Hardware->Network Adapter->Network Connection установить Bridget. Данная установка делается по умолчанию.
4. В операционной системе без сети удалить виртуальный сетевой адаптер. VM->Settings->Hardware->Network Adapter нажать Remove.
5. В хостовой операционной системе отключить сетевые протоколы IPv4 и IPv6 от физических адаптеров. Это делается в свойствах сетевых карт. Отключить только от физических сетевых карт, т.к. там еще появляются виртуальные.
6. После этого мы будем иметь доступ в сеть только из виртуальной машины.

Важно:

В случае наличия внутреннего нарушителя он может воспользоваться беспроводным USB-модемом. В настоящее время уже есть ряд USB-модемов, поддерживающих интерфейс RNDIS, для которых при активации на Windows 7 не требуется установка новых драйверов (например, Yota One или телефоны на Windows Mobile). При этом в системе появляется новая сетевая карта.

Решение данной проблемы может быть разным. Для виртуальной машины можно отключить USB. Но при этом возможно активировать данное устройство в хостовой ОС. Если это приемлемо, то можно отключить интерфейс USB. Если это не приемлемо, то надо использовать системы управления доступом к устройствам (DeviceLock, SecretNet, Secure Pack Rus.

2. Личные данные больше не секрет

Кража информации, как и любая кража, является преступлением. В середине прошлого века основными методами получения конфиденциальной информации являлись кража кошельков и бумажников, поиск обрывков бумаг в мусоре, ложные звонки от лица представителей финансовых учреждений и другие. В современном мире появились такие способы, как использование специальных устройств для считывания номеров кредитных карт и, конечно, разнообразные методы кражи информации, сохранённой в памяти и передаваемой с использованием персонального компьютера[8].

В настоящее время можно выделить как минимум три «компьютерных» способа кражи информации. В первом случае пользователь сам передаёт информацию злоумышленникам, поверив в составленный специальным образом фальшивый запрос на передачу такой информации, который обычно распространяется в виде спам-рассылки по электронной почте или в виде сообщений в социальной сети. При этом злоумышленники создают фальшивую web-страницу, имитирующую страницу реально существующего банка или другой финансовой организации. Такой тип компьютерных преступлений называется фишингом.

Второй метод кражи конфиденциальной информации основан на слежении и протоколировании действий пользователя. Такой электронный шпионаж осуществляется с помощью специальных троянских программ, называемых «троянцы-шпионы» Одним из самых популярных на данный момент классов троянских программ этого типа является класс кейлоггеров (клавиатурных шпионов), основным назначением которых является скрытое запоминание нажатий клавиш и ведение журнала этих нажатий.

Третий метод кражи конфиденциальной информации основан на использовании троянских программ для поиска и скрытой передачи собранных на компьютере пользователя конфиденциальных данных автору вредоносной

[8] http://www.kasperskyclub.ru/mainmenu-3/19/129---

программы. В этом случае злоумышленник может получить только те данные, которые сохранены на компьютере пользователя. Однако этот «недостаток» компенсируется тем, что весь процесс сбора и передачи конфиденциальной информации происходит без участия пользователя.

Получить троянские программы указанных типов можно самыми различными путями: при просмотре вредоносного сайта, по почте, в чате, форуме, через интернет-пейджер или иным способом во время путешествия по всемирной паутине. В большинстве случаев злоумышленники одновременно с вредоносными программами используют приемы социального инжиниринга, целью которых является подвигнуть пользователя к совершению необходимых киберпреступнику действий.

В качестве примера рассмотрим реальную троянскую программу Trojan-PSW.Win32.LdPinch, главной целью которой является кража паролей от различных установленных на компьютере пользователя программ. Список программ, пароли от которых может украсть LdPinch, впечатляет: Internet Explorer, Outlook Express, Mozilla Firefox, Opera, CuteFTP, FAR, The Bat!, MS Office Outlook, Mail.Ru Agent, Eudora, Mozilla Thunderbird, ICQ, Miranda, TRILLIAN, GAIM, MSN & Live Messenger и другие.

При этом украденные пароли используются и для дальнейшего распространения вредоносной программы. Так, получив пароль от клиентской программы службы ICQ, троян меняет его на сайте ICQ и начинает рассылать сообщения по контакт-листу жертвы, содержащие ссылку на собственный исполняемый файл, стараясь таким образом увеличить число заражённых машин.

Сообщения имеют вид:

Смотри<ссылка_на_вредоносную_программу> Классная вещь! :-)

Вот реальная картинка (рис.1) (вредоносная ссылка удалена), которые рассылались в социальной сети Mail.ru в разделе Мой мир.

Рис.1. Вредоносное воздействие на Mail.ru

Практически каждый получатель данного сообщения идет по вредоносной ссылке и запускает троянца. Происходит это из-за высокого уровня доверия к сообщениям от друзей. Получатель не сомневается, что сообщение пришло от его знакомого. И так по кругу: заразив компьютер вашего знакомого, троянец рассылает себя дальше по всем контакт-листам, обеспечивая автора программы ворованными пользовательскими данными.

Вся украденная информация в зашифрованном виде отсылается либо на определённый адрес электронной почты, либо выкладывается на FTP-сервер злоумышленника.

Как выглядят фишинговые письма?

В случае с фишингом никаких вредоносных программ на компьютер пользователя не загружается. Используя методы социального инжиниринга, злоумышленники настоятельно побуждают пользователя ввести свои конфиденциальные данные на специально созданной web-странице. Предлогов для этого может быть множество. Рассмотрим фишинговое письмо, рассылавшееся перед наступлением 2007 года, в частности клиентам почтовой системы Gmail (Google Mail).

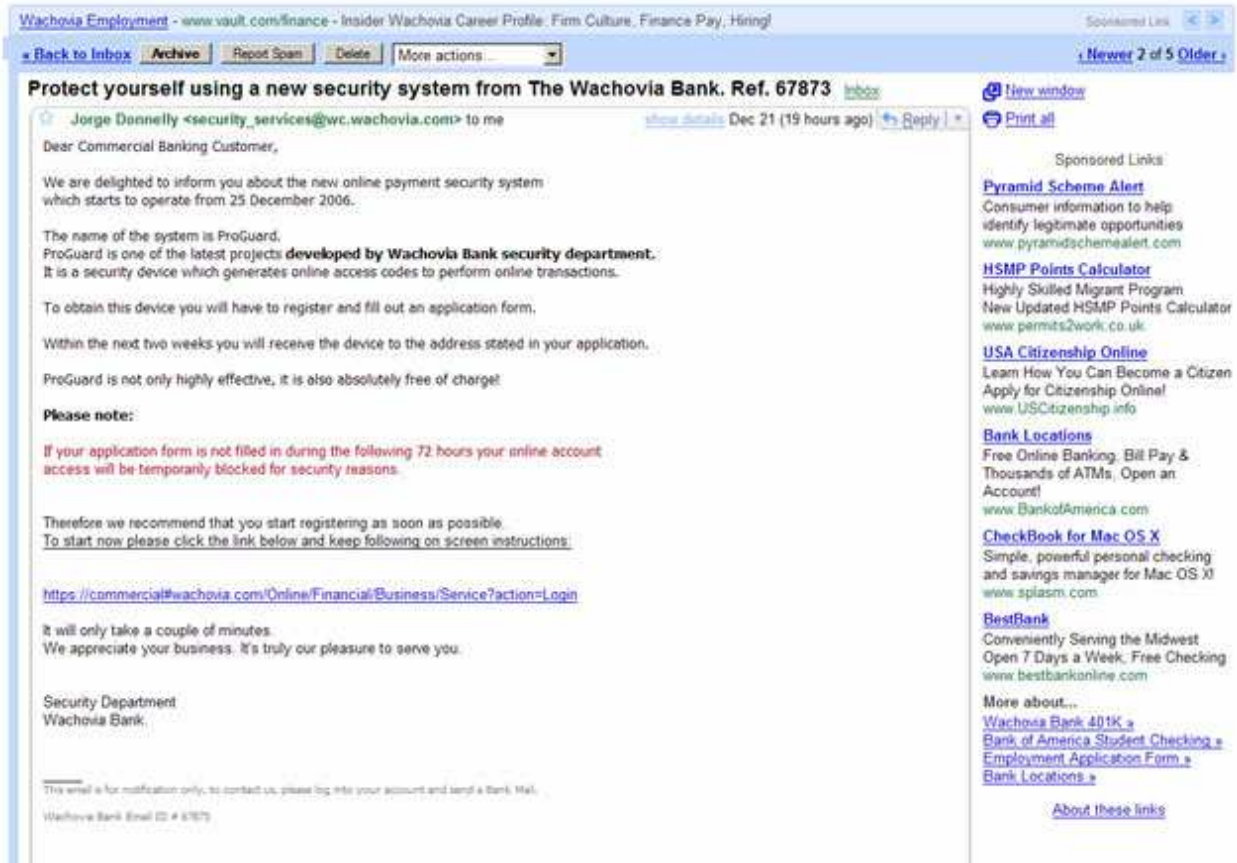

Рис.2 Пример фишингового письма

В письме сообщается, что отдел безопасности банка Wachovia разработал прибор ProGuard, предназначенный для генерации кодов доступа для выполнения банковских транзакций онлайн. Пользователю предлагается заполнить регистрационную форму, ссылка на которую указана в теле письма.

Регистрационная форма расположена на странице, очень похожей на страницу реального банка Wachovia — четвёртого по размерам банка США, головной офис которого расположен в штате Северная Каролина. Кроме этого в письме находится предупреждение, выделенное красным цветом, о том, что если форма регистрации не будет заполнена в течение 72 часов, то доступ к онлайн-счёту банка будет временно заблокирован в целях безопасности. Таким образом, злоумышленники, организовавшие данную фишинговую атаку, подталкивают клиентов банка Wachovia к заполнению формы в максимально короткие сроки. Это необходимо им потому, что в настоящее время существует несколько организаций, которые очень оперативно пополняют базы фишинговых сайтов. Например, международная антифишинговая группа www.antiphishing.org, ведущая статистику по фишинг-преступлениям, обновляет базу фишинговых URL каждые 5 минут. Базы этих организаций используются во многих продуктах защиты для детектирования фишинговых страниц и писем.

Для убеждения пользователя в истинности письма злоумышленники часто используют логотипы банка, имена и фамилии реальных руководителей банка. Приводимая в письме ссылка на страницу банка создается злоумышленниками таким образом, что на экране жертвы она отображается как реально существующий сетевой адрес сайта банка, на самом же деле ссылка при ее активации приведет на сайт злоумышленника. Появление в конце 2003 года уязвимости с подменой реального URL привело к появлению новой разновидности фишинга, получившего название «спуфинг» (spoofing). В случае использования данной уязвимости атакуемый пользователь визуально может наблюдать настоящий адрес банковского сайта даже в адресной строке браузера, но находиться сам при этом будет на сайте поддельном.

К сожалению, в приведённом выше примере можно увидеть ещё один элемент, которые может повлиять на то, что пользователь поверит присланному письму, хотя его авторы здесь и ни причём. Web-интерфейс Gmail добавил к внешнему виду письма ряд рекламных ссылок и блоков, контекстно связанных

с данным банком (они находятся в левом верхнем и правом нижнем углу скриншота). Очевидно, что наличие подобной «обертки» увеличивает доверие пользователя к письму и исполняет роль успокаивающего фактора, который может привести к тому, что человек действительно поверит злоумышленникам и посетит поддельный сайт.

Но рассмотрим пользователя, который не работает с онлайн-системами банковских платежей и не хранит никакой конфиденциальной информации на компьютере. Допустим, что основным занятием такого пользователя за компьютером является игра в онлайновые игры. Актуальна ли для него проблема кражи информации? Безусловно!

В качестве примера рассмотрим две троянские программы, предназначенные для кражи учетных записей на игровых серверах двух известных игр Lineage и World of Warcraft. Троянская программа Trojan-PSW.Win32.Lineage.agi устанавливает в системе перехватчики событий от мыши и клавиатуры, которые ищут окна браузера Internet Explorer и получают данные, введенные в полях ввода имени и пароля главной учётной записи и ряда других. Собранные данные передаются на сайт злоумышленника. Троянская программа Trojan-PSW.Win32.WOW.el использует более сложный метод: библиотека устанавливает перехватчика функции «send» из библиотеки WS2_32.dll, с помощью которого следит за HTTP запросами пользователя. При перехвате определённых запросов троянец получает значение имени учётной записи и пароля к ней. Кроме того, для основного процесса игры wow.exe троянская программа получает значения полей ввода в диалогах, а также делает скриншоты некоторых диалогов. Собранную информацию троянец также отправляет на сайт злоумышленника.

Как же можно защититься от угрозы кражи информации, связанной с использованием персонального компьютера? Существует несколько рекомендаций, причём они применимы как к персональному пользователю, так и к организациям.

Во-первых, необходимо сформировать правильное отношение к безопасности и использовать существующие средства защиты: антивирусные продукты, спам-фильтры, сетевые экраны. Для организаций эти средства желательно дополнить системами мониторинга активности и аудита сетевой инфраструктуры.

Во-вторых, поддержка базы установленного антивирусного продукта в актуальном состоянии. Это позволит противостоять известным угрозам.

В-третьих, использование средств проактивной защиты. Этот вид защиты отличается от сигнатурного (реактивного) детектирования тем, что пользователю не надо ждать, пока антивирусные аналитики добавят запись о новой угрозе в антивирусные базы, а продукт обновит базы с серверов обновлений производителя. Модуль проактивной защиты обеспечивает защиту пользователя от новых типов угроз и новых модификаций существующих вредоносных программ без обновления баз, так как его работа основана на постоянном мониторинге действий всех процессов в системе пользователя. Вердикты (опасен, подозрителен и так далее) выносятся на основе анализа этих действий.

Еще один прием — использование средства защиты конфиденциальных данных, основанных не на анализе трафика, а на мониторинге активности запущенных приложений.

Кроме того, необходимо избегать сообщения параметров своих банковских карт в сети. Если человеку необходимо совершить сетевой платеж — специалисты советуют завести отдельную карту или кошелек для этого, переводя туда деньги непосредственно перед покупкой.

Немаловажно воздерживаться от операций с интернет-магазинами, инвестиционными фондами и прочими организациями, если они расположены на доменах третьего уровня, да еще и на бесплатном хостинге. Уважающая себя организация найдет незначительную сумму на собственный домен второго уровня.

Опытный пользователь никогда не ответит на рассылки от имени банков, фондов и прочих структур просто потому, что они их не проводят. Если клиент в этом сомневается, то необходимо проверить факт рассылки по телефону. Но только не по тому, который может быть указан в теле сообщения. Ведь если письмо отправлено злоумышленником, то номер, безусловно, принадлежит ему же.

Таким образом, достаточно простые технические приемы и внимательность пользователей могут значительно снизить риск кражи, как данных, так и денег кибер злоумышленниками.

ЭТО ИНТЕРЕСНО

Атаки методом подбора пароля (Brute force attacks) — или атаки методом "грубой силы". Используя пользователями простейших паролей (например "123", "admin" и т.д) - они тем самым дают злоумышленникам возможность определить пароль методом подбора, при помощи специальных троянских программ. Данные троянские программы используют словари паролей, заложенные в эту программу, или генерируют случайные последовательности символов.

Клавиатурные перехватчики (Keyloggers) — вид троянских программ, основной функцией которых является перехват данных, вводимых пользователем через клавиатуру. Объектами похищения являются персональные и сетевые пароли доступа, логины, данные кредитных карт и другая персональная информация.

Люки (Backdoors) — программы, обеспечивающие вход в систему или получение привилегированной функции (режима работы) в обход существующей системы полномочий. Часто используются для обхода существующей системы безопасности. Люки не инфицируют файлы, но прописывают себя в реестр, модифицируя, таким образом, ключи реестра.

Сниффинг (Sniffing) — вид сетевой атаки, еще называется "пассивное прослушивание сети". Несанкционированное прослушивание сети и наблюдение за данными производятся при помощи специальной не

вредоносной программой - пакетным сниффером, осуществляющим перехват всех сетевых пакетов домена, за которым идет наблюдение. Перехваченные таким сниффером данные могут быть использованы злоумышленниками для легального проникновения в сеть на правах фальшивого пользователя.

Фарминг (Farming) — позволяет изменять DNS (Domain Name System) записи либо записи в файле HOSTS. При посещении пользователем легитимной, с его точки зрения, страницы производится перенаправление на поддельную страницу, созданную для сбора конфиденциальной информации. Чаще всего такие страницы подменяют страницы банков – как оффлайновых, так и онлайновых.

Бомбы с часовыми механизмами (Time bombs) — одна из разновидностей логических бомб, в которых срабатывание скрытого модуля определяется временем.

DoS-атаки (DoS-attacks) — или атаки на отказ в обслуживании. Популярный у злоумышленников вид сетевых атак, граничащий с терроризмом, заключающийся в посылке огромного числа запросов с требованием услуги на атакуемый сервер с целью выведения его из строя. При достижении определенного количества запросов (ограниченного аппаратными возможностями сервера), последний не справляется с такими запросами, что приводит к отказу в обслуживании. Как правило, такой атаке предшествует спуфинг. DoS-атаки стали широко используемым средством запугивания и шантажа конкурентов.

Почтовые бомбы (Mail bombs) — один из простейших видов сетевых атак. На компьютер пользователя или почтовый сервер компании посылается одно огромное сообщение, или множество (десятки тысяч) почтовых сообщений, что приводит к выводу системы из строя.

Спуфинг (Spoofing) — вид сетевой атаки, заключающейся в получении обманным путем доступа в сеть посредством имитации соединения. Используется для обхода систем управления доступом на основе IP адресов, а

также для набирающей сейчас обороты маскировки ложных сайтов под их легальных двойников или просто под законные бизнесы.

Вишинг (Vishing) — технология интернет-мошенничества, разновидность фишинга, заключающаяся в использовании в злонамеренных целях "war diallers" (автонабирателей) и возможностей Интернет-телефонии (VoIP) для кражи личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д. Потенциальные жертвы получают телефонные звонки, якобы от имени легальных организаций, в которых их просят ввести с клавиатуры телефона, смартфона или планшета пароли, PIN-коды и другую личную информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы и в других преступлениях.

Зомби (Zombies) — маленькие компьютерные программы, разносимые по сети Интернет компьютерными червями. Программы-зомби устанавливают себя в пораженной системе и ждут дальнейших команд к действию.

Руткит (Rootkit) — вредоносная программа, предназначенная для перехвата системных функций операционной системы (API) с целью сокрытия своего присутствия в системе. Кроме того, Rootkit может маскировать процессы других программ, различные ключи реестра, папки, файлы. Rootkit распространяются как самостоятельные программы, и как дополнительные компоненты в составе иных вредоносных программ - программ-люков (backdoor), почтовых червей и т.д.

Троянские кони (Trojan Horses) — вредоносные программы, содержащие скрытый модуль, осуществляющий несанкционированные пользователем действия в компьютере. Эти действия не обязательно будут разрушительными, но они всегда направлены во вред пользователю. Название этого типа атак происходит от известной легенды о деревянной статуе коня, использованной греками для проникновения в Трою.

Дифейсмент (Defacement) — искажение веб-страниц. Вид компьютерного вандализма, иногда являющийся для хакера забавой, а иногда

средством выражения политических или иных пристрастий. Искажения могут производиться в какой-то части сайта или выражаться в полной замене существующих на сайте страниц (чаще всего, стартовой).

Логические бомбы (Logic bombs) — вид Троянского коня - скрытые модули, встроенные в ранее разработанную и широко используемую программу. Логические бомбы являются средством компьютерного саботажа.Такой модуль является безвредным до определенного события, при наступлении которого он срабатывает (нажатие пользователем определенных кнопок клавиатуры, изменение в файле или наступление определенной даты или времени).

Фишинг (Phishing) — технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д. При помощи спамерских рассылок или почтовых червей, потенциальным жертвам рассылаются подложные письма (якобы от имени легальных организаций), в которых их просят зайти на подделанный преступниками "сайт" такого учреждения и подтвердить пароли, PIN-коды и другую личную информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы и в других преступлениях.

СОВЕТ: Вынесите все критичные и личные данные на отдельный внешний носитель и никогда не подключайте его к компьютеру при работе в соцсети.

3. Виртуальный Чикатило

СОВЕТ: При общении в социальной сети ведите себя вежливо и корректно, вы не можете точно знать, кто ваш собеседник или сетевой друг. Будьте готовы, что ваш собеседник вполне может оказаться не тем, за кого выдает себя в виртуальном мире. По возможности спокойно относитесь к негативной реакции на Вас, не вступайте в споры и взаимные оскорбления, помните – это может быть провокация!

Чтобы сразу обозначить проблему, которую мы рассматриваем в этой главе, приведем яркий пример имперсонации в социальной сети, когда участник общения выдает себя за другого. В данном случае пользователь Блогов Mail.ru поступает избыточно честно, раскрывая свое истинное лицо и имя.

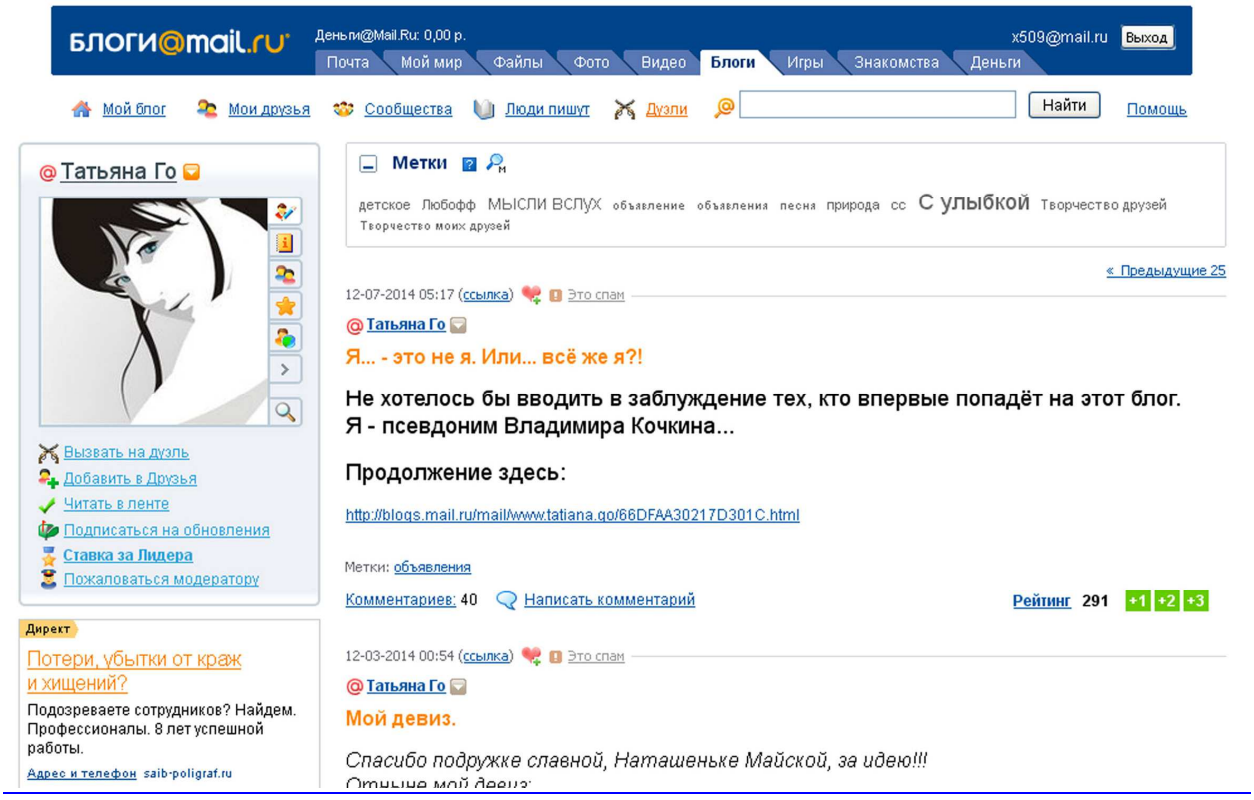

Рис.1 – яркий пример имперсонации

Потребность в параллельной виртуальной жизни[9] носит массовый характер и не может не вызывать интерес и даже иногда тревогу у психологов, социологов, педагогов и других специалистов. Виртуальная жизнь имеет свои особенности и законы и отражается на развитии реальной личности.

У пользователей социальных сетей можно выделить общие психологические особенности, которые располагают к формированию компьютерной зависимости от виртуальной реальности. Эти черты становятся общими для большинства граждан нашей страны и дают возможность говорить о тенденциях к формированию нового образа современного гражданина.

Проблема развития компьютерной зависимости от социальных сетей, неразрывно связана с особенностями личностного развития пользователя и его социального окружения в реальном мире. По данным исследований канадских ученых активные пользователи социальных сетей – это люди неуверенные в себе, обладающие низкой самооценкой, склонные к нарциссизму. Они имеют высокие баллы по тесту самовлюбленность. В социальных сетях 49% мужчин и 63% женщин: мужчины чаще публикуют разного рода заметки, тем самым привлекая внимание к своей социальной сущности; женщины больше внимания уделяют своим фотографиям. Те и другие стремятся произвести впечатление друг на друга. В данном случае подсознательно ставка делается на силу мужчины (в современном мире сильный мужчина – это социально успешный мужчина), который способен защитить женщину и потомство, и на красоту женщины, как символ здоровья, которая способна родить здоровое потомство. Женщины общаются в социальных сетях чаще, чем мужчины. Самые активные пользователи социальных сетей – это люди от 40 лет. В среднем они отправляют более 10 писем в день. Мужчины, состоящие в браке, пользуются услугами Интернет - общения чаще, чем холостяки. Использование социальных сетей, по мнению психологов, напоминает рассматривание себя в зеркало.

[9] УДК 316.6 ПСИХОЛОГИЧЕСКИЙ ПОРТРЕТ АКТИВНОГО ПОЛЬЗОВАТЕЛЯ СОЦИАЛЬНЫХ СЕТЕЙ Е.А.Шайкина http://archive.nbuv.gov.ua/portal/soc_gum/domtp/2011_4/Wajkina.pdf

Личная страница пользователя социального сайта с позиции популярной психологии – это представление своей социальной принадлежности. Эта страница является проекцией личности, информационным портретом, и может служить основанием для составления психологического портрета ее владельца. Человек, который заводит страницу в социальной сети, опирается на образ, способный вызвать желаемое мнение о нем у посторонних людей. Образ, как правило, подбирается так, чтобы получить признание окружающих. Сетевой облик пользователя складывается из частоты размещения фотографий, частоты обновления статуса и информации на стене, частоты и длительности сессии. В ходе исследования мы выявили личностные особенности пользователей, склонных к зависимости от социальных сетей. Первая характеристика, на которую хотелось бы обратить внимание – это неуверенность в себе. Этим качеством, как показала практика, обладают люди с разным социальным статусом. Чувство неуверенности может касаться различных сторон жизни: недостаток социального признания, сексуальная несостоятельность, комплексы в личностном развитии, проблемы в общении и т.д. Анонимность в Интернете позволяет быть раскрепощенным, попробовать себя в новой социальной роли, пренебречь нормами общественной морали, выстраивать и разрывать отношения, не думая о последствиях. Часто такие пользователи утверждаются за счет других. Сильный человек утверждается в реальном мире, ему не нужна компенсация. Она ничего не дает ему сверх того, что он уже имеет. Для неуверенных пользователей социальные сети – это решение многих проблем. Забыв свои комплексы, они раскрепощаются, и, в конечном итоге, это позволяет им повысить свою самооценку. Однако подобное решение этой проблемы порождает другую проблему – ученые Стендфортского университета утверждают, что нахождение в социальной сети может сделать пользователя несчастным человеком. В Интернете люди склонны приукрашивать свою жизнь, поэтому не всегда выкладывается достоверная информация: фотографии, сделанные во время отдыха и самые удачные, сообщения только о своих достижениях, преувеличенный социальный статус и т.д. Создается

впечатление, что у всех благополучная жизнь и достаток (по статистике 70% пользователей верят, что все написанное – правда). На этом фоне свои проблемы кажутся более значительными и непреодолимыми, что может привести к депрессии. Следует очень критично относиться к информации, которая выкладывается в социальных сетях, т.к. следующая черта личности, характеризующая активного пользователя – это демонстративность. Такие люди не желают заявлять о своих проблемах публично. Они говорят только о своих достоинствах, при том преувеличивают их. Страницы демонстративных пользователей отличаются большим количеством индивидуальных фотографий, на которых они в выгодном ракурсе. В зависимость от социальных сетей попадают люди со слабой силой воли. Такой личности трудно найти свое место в реальном мире и она пытается найти его в виртуальном. Она находит это в суррогатном виде. Виртуальное общение необходимо им для самоутверждения. Оно удобно, т.к. в виртуальном мире отсутствует острая борьба мотивов, можно переиграть любой жизненный сценарий без последствий. Социальные сети – это выход для пользователей с проблемами в общении: появляются противоречия между желанием общаться и умением устанавливать контакты, а главное – сохранять отношения. Такие люди не могут выстроить и сохранить контакты в реальности, поэтому они уходят в виртуальный мир, в котором общение ни к чему не обязывает, контакт может быть прерван без всяких объяснений нажатием кнопки. Самооценка активных пользователей социальных сетей, как правило, занижена, при этом отмечается достаточно высокий уровень самовлюбленности. Психологам хорошо известно, что у самовлюбленных людей возникают большие проблемы с выстраиванием долговременных близких отношений и у них низкий уровень эмпатии. При этом из-за низкой самооценки человек не уверен в себе, боится попасть в психологически некомфортную для себя ситуацию. Такой личности проще найти себя в виртуальной реальности, где общение не требует живых эмоций и переживаний, а анонимность обеспечивает психологическую защиту. В ходе исследования выделены личностные качества пользователя, склонного к

формированию компьютерной зависимости от социальных сетей. Характеристика такой личности включает в себя заниженную самооценку при достаточно высоком уровне самовлюбленности, неразвитую силу воли, неуверенность в себе, наличие больших проблем в общении, низкий уровень эмпатии. Уход от реальных проблем в виртуальный мир не спасает человека от психологического дискомфорта. Такой уход может только предоставить временную суррогатную замену. Дискомфорт в реальности связан с наличием проблем в развитии личности и решать эту проблему можно только путем достижения ее гармоничного развития. Основным же условием психологического благополучия любого человека является соответствие внутреннего мироощущения личности ее социальной сущности.

Но наш читатель, конечно, не такой. Написанное выше – всего лишь попытка предостеречь от разочарований сетевого общения и сетевых отношений, поэтому будьте корректны и осторожны в общении и не обижайтесь на не всегда адекватные реакции со стороны психологически проблемных пользователей соцсетей.

Поговорим немного о такой угрозе, как кибермоббинг — это термин, пришедший (от англ. Cyber-Mobbing) английского языка, также *Интернет-моббинг* (*Internet-mobbing*), *кибербуллинг* (*Cyberbullying*), под которым понимают намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени.

Кибермоббинг осуществляется в информационном пространстве через информационно-коммуникационные каналы и средства. В том числе в Интернете посредством электронной почты, программ для мгновенного обмена сообщениями (Instant Messenger, например ICQ) в социальных сетях, а также через размещения на видеопорталах (YouTube, Vimeo других) непристойных видеоматериалов, либо посредством мобильного телефона (например, с помощью SMS-сообщений или надоедливых звонков).

Лица, совершающие данные хулиганские действия, — которых часто называют «Булли» или «Мобберы» — действуют анонимно, так что жертва не знает, от кого проистекают агрессивные действия.

Основные отличия кибермоббинга от *традиционного моббинга*

Обычно под моббингом понимают групповой психологический террор в виде косвенной или прямой травли сотрудника в коллективе, как правило, с целью его увольнения.

В широком смысле моббинг представляет собой систематическое, повторяющееся в течение длительного времени третирование, оскорбление, унижение достоинства другого человека, например, в школе, на рабочем месте, в тюрьме, и через Интернет (кибермоббинг), и так далее. Типичные действия, осуществляемые при моббинге — это распространение заведомо ложной информации (слухов и сплетней) о человеке, насмешки и провокации, прямые оскорбления и запугивание, социальная изоляция (бойкот и демонстративное игнорирование), нападки ущемляющие честь и достоинство человека, причинение материального или физического вреда.

К формам психологического давления присущего традиционному моббингу добавляются возможности всемирной паутины, благодаря чему кибермоббинг приобретает следующие функции:

- Круглосуточное вмешательство в личную жизнь. Кибермоббинг не имеет временного или географического ограничения. Нападки не заканчивается после школы или рабочего дня. Киберхулиган (моббер) круглосуточно имеет прямой доступ через технические средства к жертве: мобильный телефон или профиль в социальных сетях и электронная почта. Благодаря интернету жертва не защищена от моббинг-атак и дома.
- Неограниченность аудитории, быстрота распространения информации. Сообщения или изображения, пересылаемые электронными техническими средствами, очень трудно контролировать, как только они оказались онлайн. Например, видео легко копируются с одного интернет-портала на другой. Поэтому размер аудитории и поле распространения

кибермоббинга гораздо шире «обычного» моббинга. Тот контент, о котором уже давно забыли, может вновь попасть на глаза общественности, и жертве будет трудно его нейтрализовать.

- Анонимность Кибермоббера. Киберпреступник не показывает себя своей жертве, может действовать анонимно, что обеспечивает ему — пусть и кажущуюся — безопасность и нередко увеличивает срок его негативной «кибер-активности». Незнание жертвы, кем является тот, «другой», кто её третирует, может запугать её и лишить покоя.

Люди, и в частности дети, которые стали жертвами кибермоббинга в Интернете, как правило, уже ранее были целью моббинга в реальной жизни. В большинстве случаев, основной удар кибермоббера приходится на внешний вид, на «аватар» подростка или взрослого (например, слишком худой или слишком толстый и так далее).

Основное количество жертв и мобберов приходится на возраст между 11-16 годами — пубертатный период, характеризующийся высокой чувствительностью к любым оскорблениям, слухам и социальным неудачам.

Это не играет роли, научены ли подростки обращаться с конфликтами, уметь выходить из конфликтной ситуации, активно обороняться или имеют широкий круг друзей, которые могут их поддержать. В действительности мы наблюдаем, что наиболее социально адаптированные и приспособленные ученики, которые избегают конфликтов, очень легко могут стать целью кибермоббинга. Терапия при сложных нарушениях может длиться около 3-х месяцев. Основная цель терапии — заново помочь создать положительное социальное окружение, в котором дети себя будут чувствовать полноценно, освободить их от цепей социальной изоляции. Длительное воздействие на ребёнка кибер-террора приводит к сильному нарушению его самооценки и чувства собственного достоинства. Ужасающее воздействие такого нового феномена, как кибермоббинг вызвало к жизни различные общественные и государственные инициативы для поддержки развития у детей медиакомпетенций и запуску превентивных проектов, направленных против

кибермоббинга. Так в 2009 году в Евросоюзе была запущена „Safer Internet Programme“ ,) в которой участвуют 26 стран ЕС.

Зачастую жертвы не могут получить адекватную помощь от родителей или учителей, так как до сих пор последние не владеют опытом и знанием о данной проблематике.

Кибермобберы

В осуществлении кибер-террора участвует примерно равное количество мальчиков и девочек. Исследование 2008 года показало, что 16 % из опрошенных людей сами когда-либо занимались кибермоббингом в Интернете, а 40 % из них воспринимали данное действие как шутку, проделку.

Формы киббермоббинга по классификации Нэнси Виллард (Willard, 2007)

- Flaming (Флэминг, оскорбление). Как правило, происходит в открытом публичном пространстве Интернета, посредством оскорбительных комментариев, вульгарных обращений и замечаний.
- Harassment (Харрасмент, домогательство). Целенаправленные, систематические кибер-атаки от незнакомых людей, пользователей социальных сетей, людей из ближайшего реального социального окружения.
- Denigration (Денигрэйшн, очернение, распространение слухов). Намеренное выставление жертвы в чёрном свете с помощью публикации на Интернет страницах, на форумах, в новостных группах, через E-Mail текстов, фото/видео материалов, например, чтобы разрушить дружеские отношения или отомстить экс-подруге.
- Impersonation (Имперсонация, использование фиктивного имени). Намеренно выдавать себя за другого человека, используя пароль жертвы, например, для того чтобы оскорбить учителя.
- Outing and Trickery (публичное разглашение личной информации). Распространение личной информации, например, интимных фотографий, финансового положения, рода деятельности с целью оскорбить или шантажировать, например, экс-партнера.

- Exclusion (социальная изоляция). Отказ общаться (как на деловом, так и на неформальном уровне), исключение из Instant-Messenger группы или игрового сообщества и так далее.
- Cyberstalking (Кибersталкинг, продолжительное домогательство и преследование). Систематическое (сексуальное) преследование кого-либо, сопровождающееся угрозами и домогательствами.
- Cyberthreats (открытая угроза физической расправы). Прямые или косвенные угрозы убийства кого-либо или причинения телесных повреждений.

Причины кибермоббинга

- Страх: чтобы не стать жертвой моббинга чаще примыкают к активной, предположительно сильной группе коллектива.
- Завоевание признания: потребность «выделиться», быть на виду, завоевать влияние и престиж в группе.
- Межкультурные конфликты: национальные различия в культуре, в традициях, в языке, нетипичная внешность.
- Скука: например, от скуки негативно прокомментировать чью-либо фотографию.
- Демонстрация силы: потребность показать свое превосходство.
- Комплекс неполноценности: возможность «уклоняться» от комплекса или проецировать его на другого. Большая вероятность стать причиной насмешек из-за чувства своей ущербности.
- Личностный кризис: разрыв любовных отношений, дружбы, чувство ненависти и зависти, неудачи, провалы, ошибки.

Кибермоббинг в учебном заведении

Учителям не всегда просто удается вовремя обнаружить случаи кибермоббинга в школе на этапе их возникновения. Как правило, учителя узнают о случае кибермоббинга достаточно поздно, на этапе эскалации конфликта. Упреждающие меры по узнаванию кибер-террора в школе могут способствовать смягчению конфликта и препятствуют его распространению.

Возможные признаки кибермоббинга в школе:

- Анонимность «почтового ящика». Ученики с помощью своего почтового ящика получают возможность осуществлять кибермоббинг анонимно. Необходимо учитывать тот факт, что эти анонимные почтовые ящики могут быть использованы для травли других учеников.
- Ухудшение психологического климата в классе. Если отношения между учениками в классе все чаще приобретают недружественный характер, увеличивается частота конфликтов, то это способствует развитию кибермоббинга.
- Разрыв дружественных связей между учениками. Особенно чувствительно переживается разрыв дружбы между девочками, когда бывшая подруга становится объектом кибер-террора любимой подруги, так как они знают друг о друге много личной информации и стараются её использовать друг против друга.
- Школьные мероприятия. Во время различных школьных мероприятий: экскурсионные поездки, праздники, конкурсы, спортивные состязания становится видно, насколько сплочен классный коллектив, становится осязаемой «линия надлома» межличностных отношений внутри класса.

Симптомы, проявляющиеся у жертв кибермоббинга

- Ухудшение показателей здоровья. Сюда могут относиться такие симптомы, как головная боль, боль в животе, проблемы со сном, подавленное настроение.
- Изменение поведения. Сигналом для тревоги может послужить неожиданная замкнутость и закрытость ученика, снижение успеваемости в школе, отстраненность от реального мира, частое пребывание в мире фантазий и в мире онлайн-игр.
- Пропажа личных вещей ученика. Неожиданное исчезновение любимых вещей ученика и денег, которое легко могут заметить родители.
- Недооценка серьезности и умаление значения кибер-террора. Жертвы моббинга на первом этапе общения со взрослыми зачастую скрывают

случаи кибер-травли, которые осуществляют с ними другие ученики или умаляют их значение в глазах взрослых. Если есть серьезные подозрения на наличие кибер-террора, необходимо провести повторную беседу с учеником и усилить наблюдение за ним.

Защита от кибермоббинга

Как только кто-то становится жертвой кибермоббинга, так сразу к нему приходит ощущение полной беспомощности. Словесные аргументы или просьбы оставить в покое не имеют шансов в борьбе с анонимной кибермоббинг группой. Низкая самооценка жертвы обостряет ситуацию отчаяния и беспомощности. Оставшись «наедине» с кибермобберами, трудно ожидать помощи или поддержки со стороны: если негативное видео попало в сеть, то за короткий период времени оно наберет большое количество просмотров. Как следствием может стать незамедлительная социальная стигматизация жертвы.

Родители должны подробно расспросить ребёнка о случившемся прецеденте моббинга и информировать о нём школу. Взрослые могут также помогать детям и подросткам в противостоянии кибертеррору: например, могут сообщить в правоохранительные органы, выступить в качестве медиатора в разрешении конфликта.

Совершенствование знаний и понимания в области медиакомптенций родителей, педагогов и воспитателей — лучшая профилактика в борьбе с кибермоббингом.

Реакция на кибермоббинг

Быстрые и превентивные действия против моббинга смягчают, а в лучшем случае предотвращают эскалацию конфликта.

Большинство жертв не отваживается обратиться за помощью и предать огласке их травлю, потому что боятся оказаться полностью изолированными от социального окружения.

Первая помощь, помощь самому себе при кибермоббинге

Повсюду в цифровом мире, как и в реальной действительности, распространяется принцип всеобщей ответственности: все люди ответственны за то, что они смотрят, что они делают, что они публикуют в Интернете.

Также существует группа в социальной сети Вконтакте.ру «Анти-КиберМоббинг» (Anticybermobbing). В которой можно получить консультацию в реальном времени.

В Москве существует бесплатная служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования интернета «Дети онлайн» — 8-800-25-000-15 с 9 до 18 МСК по рабочим дням. На Линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М. В. Ломоносова и Фонда Развития Интернет.

Использование современных коммуникационных технологий для Кибермоббинга

Технологии	**Позитивное использование**	**Возможные злоупотребления**
Мобильные телефоны	1.Общение с помощью текста и картинок 2.Картинки и фильмы снимать и отправлять 3.Слушать музыку 4.Играть 5.Пользоваться Интернетом 6.Писать E-Mails? 7.Предоставить ребёнку больше независимости и возможность использовать мобильный телефон при ЧС	1.Систематически осуществлять анонимные звонки и сообщать негативные сообщения (угрозы, запугивания, оскорбления). 2. Делать компрометирующее видео и фото, публиковать их в Интернете (например, Happy Slapping)
Instant Messenger(IM)	1.Общаться с друзьями в чате (писать или разговаривать)	1. Рассылать подлые сообщения, картинки или видео

	2.Быстрая и эффективная возможность оставаться на связи	2. Использовать другой аккаунт, чтобы писать негативные сообщения людям из контакт-листа.
Чат	1. Люди со всего мира могут обсуждать общие темы в группах. 2. Хорошая возможность для знакомства с другими людьми	1. Отправлять анонимные угрозы или оскорбления. 2. Создание групп, в которых намеренно игнорируются определенные люди. 3. Выстраивание фальшивых дружеских или родственных отношений (чтобы узнать личную, интимную информацию). Возможные последствия: распространение слухов, психологический террор.
E-Mail	1.Электронные письма, картинки, сведения быстро и эффективно отправлять в любую точку мира.	1. Рассылать злые и негативные сообщения. 2. Рассылать непристойные материалы (видео, картинки или компьютерные вирусы). 3. Взлом другого аккаунта, для использования личного E-Mail для рассылки различной информации или для его удаления.
Веб-камера	1.Делать фото и снимать видео. 2.Видеть другого человека на экране и вести с ним диалог. 3.Проводить видеоконференции.	1.Непристойное видео снимать и рассылать. 2. Убеждать или принуждать молодых людей к непристойным действиям. 3. Публиковать в Интернете личные фото и видео материалы после расставания, чтобы опозорить экс-

		друга/экс-подругу.
Социальные сети	1.Вступать в контакты с друзьями, знакомится с новыми людьми, назначать встречи. 2. Возможность креативно проявлять себя в Интернете, например, публиковать свои музыкальные сочинения. 3.Создавать свой личный профиль и свою домашнюю страницу, редактировать её содержание.	1. Писать обидные комментарии к фотографиям, к видео, на стене пользователя, в сообществах. 2. Распространять непристойное видео и фото. 3. Взлом чужого аккаунта, редактирование его с целью очернить другого человека (например, рассылка сообщений с этого аккаунта, дополнение лживой информации). 4. Намеренное создание группы, для выражения ненависти и травли определенного человека. 5. Создание фальшивого профиля для третирования другого человека.
Видео-порталы	1.Скачивать интересное и развлекательное видео, загружать свое видео.	1.Непристойное, компрометирующее, позорящее другого человека видео публиковать в Интернете. 2. Личные фотографии (в основном эротического содержания) после разрыва отношений публиковать в Интернете с целью досадить бывшему партнеру/партнерше.
Система управления обучением	1. Помощь для самостоятельного обучения. 2. Предоставление учебных материалов, домашних заданий, рефератов.	1.Писать непристойные новости.
Игровые порталы, виртуальные	1.Во время онлайн-игр	1.Опытные игроки заведомо

миры(например Worldof Warcraft)	общаться с геймерами всего мира (письменно и устно). 2. Виртуальные миры позволяют пользователям создавать свои аватары, которые репрезентируют их авторов другим пользователям в виртуальном мире.	выбирают себе слабых соперников и убивают их персонажей. 2. Намеренное удаление игрока из группы или игровых событий.

ЭТО ИНТЕРЕСНО

Законодатели штата Аризона одобрили поправки в закон[10], запрещающие «троллинг» в Интернете. По словам законодателей, цель инициативы состоит в том, чтобы покончить с киберзапугиванием и нецензурной лексикой в сети, объявив это вне закона.

Против нового закона уже выступила коалиция СМИ — организация, объединяющая представителей кино- и музыкальной индустрии.

В письме на имя губернатора Аризоны противники нового закона заявляют, что он может криминализировать всю интернет-аудиторию, поскольку его формулировки, по мнению авторов письма, слишком расплывчаты.

Отметим, что бурные и провокационные дискуссии в Интернете заинтересовали даже учёных. Сотрудники Северо-Западного университета в США провели исследование получившего большое распространение в наши дни такого явления, как «троллинг».

Они пришли к выводу, что анонимность доставляет веб-пользователям чувство эйфории, схожее с алкогольным опьянением или чувством власти.

Под «троллингом» понимается использование во время дискуссий в Интернете провокационных или грубых заявлений, нацеленных на создание конфликтов между участниками диалога.

[10] http://eterra.info/mosaic/trolling-pod-zapretom

4. Чужое, непонятное, массовое

СОВЕТ: По возможности не участвуйте в сетевых акциях, не рассылайте чужих сообщений, даже если вас подвигают на это идеи сострадания и гуманизма - эта пересылка может содержать скрытую манипулятивную или рекламную информацию. Также не участвуйте в массовых акциях, если их организаторы вам не известны.

Десять стратегий психологического манипулирования [11] в социальной сети

1. Отвлечение внимания. Базовым элементом социального контроля является стратегия отвлечения. Цель — отвлечь внимание общественности от важных вопросов, решаемых политическими и экономическими элитами, с помощью технологии «наводнения» или «затопления» непрерывными отвлечением и незначительной информацией. Стратегия отвлечения важна, чтобы не дать гражданам возможности получать важные знания в области науки, экономики, психологии, нейробиологии и кибернетики.

2. Создать проблему — предложить решение. Этот метод также называют «проблема-реакция-решение». Создается проблема, «ситуация», вызывающая определенную реакцию общественности — чтобы люди сами начали желать ее решения. Например, допустить рост насилия в городах или организовать кровавые теракты для того, чтобы граждане потребовали принятия законов об усилении мер безопасности и проведения политики, ограничивающей гражданские свободы.

3. Стратегия постепенности. Чтобы внедрить непопулярные решения, нужно просто применять их постепенно, капля за каплей, годами. Именно так были навязаны принципиально новые социально-экономические условия (неолиберализм) в 80-х и 90-х годах: ограничение роли государства, приватизация, ненадежность, гибкость, массовая безработица, заработная

[11] http://www.inpearls.ru/comments/234173

плата, которая уже не обеспечивает достойную жизнь. То есть все те, изменения, которые при одновременном внедрении вызвали бы революцию.

4. Стратегия откладывания. Еще один способ принять непопулярные решения, это представить их как «болезненные и необходимые» и добиться в данный момент согласия граждан на их осуществление в будущем.

5. Заигрывание с народом. Большинство рекламы, которая направлена на широкую публику, пользуется языком, аргументами, символами и, особенно, интонациями, рассчитанными на детей. Будто зритель очень маленький ребенок или имеет умственную недоразвитость. Почему? «Если вы обращаетесь к адресату, будто ему 12 лет или менее, то согласно законам восприятия есть вероятность, что он будет отвечать или реагировать некритично — как ребенок».

6. Больше эмоций, чем размышлений. Использование эмоционального аспекта — это классическая технология для блокирования рационального анализа и критического восприятия индивидуумов. Кроме того, использование эмоционального фактора позволяет открыть дверь в подсознательное, чтобы доставлять туда мысли, желания, страхи, опасения, принуждение или нужные модели поведения.

7. Держать людей в невежестве и посредственности. Создание зависимого общества, неспособного к пониманию технологий и методы социального контроля и угнетения. «Качество образования, предоставляемого низшим общественным классам, должно быть как можно скуднее и посредственнее, чтобы разрыв невежества между низшими и высшими социальными классами оставался и его невозможно было преодолеть».

8. Побуждать массы увлекаться посредственностью. Внедрять в массы мысль, что модно быть тупым, пошлым и невоспитанным.

9. Усиливать чувство вины. Сделать так, чтобы индивидуумы считали, что они сами виноваты в своих бедах и неудачах из-за недостатка интеллекта, способностей, или усилий. Таким образом, вместо того, чтобы восстать против

существующей системы, индивидуумы чувствуют себя беспомощными, занимаются самоедством. Это приводит к депрессивному состоянию, эффективно способствует сдерживанию действий человека.

10. Знать о людях больше, чем они о себе. В течение последних 50 лет научные достижения привели к стремительному росту разрыва в знаниях между основной массой общества и теми, кто принадлежит к правящим элитам или используется ими. Благодаря биологии, нейробиологии и прикладной психологии, «система» пользуется передовыми знаниями о человеческом существе, то физически или психологически. Это означает, что в большинстве случаев, «система» имеет больше контроля и больше власти над индивидуумами, чем индивидуумы над собой.

5. Наш сетевой Брут…, нет – друг!

Совет: С осторожностью относитесь к выбору сетевых друзей, собеседник, не называющий своего настоящего имени, должен вызывать особую осторожность. Соблюдайте правила корректного поведения при публикации, переписке и общении. Старайтесь не использовать ненормативной лексики, не задевать ничьих убеждение, чувств и верований.

ЭТО ИНТЕРЕСНО

Отныне пользователи Интернета в Китае[12] должны регистрироваться на интернет-сайтах под своими настоящими именами. Соответствующие правила утвердил сегодня Постоянный комитет Всекитайского собрания народных представителей.

Как утверждается, данная мера направлена на обеспечение безопасности информации в Интернете, защиту законных прав и интересов граждан, учреждений и организаций, а также защиту национальной безопасности и общественных интересов.

В правилах, состоящих из 12 пунктов, излагается политика по идентификации пользователей в их отношениях с провайдерами услуг, включая телекоммуникационных операторов.

В начале 2007 года основатель издательского дома O ' Reilly Media и изобретатель термина Web 2.0 Тим O'Рейли вместе с разработчиком общедоступной энциклопедии Wikipedia Джимми Уэйлсом объявил о создании кодекса поведения для блоггеров-Blogger ' s Code of Conduct[13] , свода правил, по которым блоггерам будет рекомендовано вести дискуссии и спорить.

[12] http://eterra.info/mosaic/kitay-niki-pod-zapretom

[13] http://it-labs.narod.ru/part10.htm

Свой призыв к блоггерам всего мира выработать удобные и несложные правила, регламентирующие допустимые моральные рамки как для самих постов, так и для комментариев к ним, О'Рейли огласил после случая с его коллегой и подругой Кэти Сиерра (Kathy Sierra), по блогу которой прокатилась волна грубых оскорблений и угроз. Сформулированные им правила в большинстве своем уже давно известны сетевой общественности, но сторонники разумного поведения в Интернете получили очередной повод для высказывания своих позиций.

Например, в новых правилах категорически запрещается Интернет-ругань, в то время как ранее перебранки (так называемые флэймы) не запрещались, а, наоборот, поощрялись и назывались одним из неотъемлемых элементов общения в Сети. Если 30 лет назад главным врагом считался злобный модератор или сисадмин, который не давал ругаться и вообще злоупотреблял своим служебным положением, то на сегодняшний день, по мнению О'Рейли, главной угрозой сообщества являются сетевые писатели, которым надо всячески напоминать, кто хозяин того или иного ресурса либо блога.

Не было раньше и призывов сообща бороться с излишне эмоциональными обидчиками с перспективой обращения к помощи правоохранительных органов, так как в начале 90-х годов такое никому и в голову прийти не могло. Не было и призывов к ограничению анонимности - по той простой причине, что форумы и конференции 90-х не имели средств для анонимных ответов и максимум, на что могли рассчитывать любители анонимности, - это сетевой псевдоним.

На страницах своего блога Тим О'Рейли опубликовал черновик “Кодекса поведения блоггера” (http ://radar.oreilly.com/archives/2007/03/call_for_a_blog_1.html) и даже придумал значок (см. рис. 1), показывающий, что блог придерживается этого кодекса.

Рис. 1. Значок поддержки "Кодекса поведения блоггера" Тима О'Рейли

Для тех же сайтов, которые не пожелают соблюдать "Кодекс поведения блоггера", Тим О'Рейли предлагает значок "Свободной зоны" (anything goes) представленный на рис. 2, который предупреждал бы пользователя, что тот входит в открытую и никем не контролируемую зону.

Рис. 2. Значок сайтов без поддержки "Кодекса поведения блоггера" Тима О'Рейли

Джимми Уэйлс, в свою очередь, приглашает всех внести свой вклад в разработку таких правил на страницах Wikipedia[14]

На время подготовки данной статьи вариантов правил было много, а последняя редакция в Wikipedia выглядит следующим образом:

- Отвечать за свои слова и ограничивать высказывания, которые не соответствуют базовым правилам вежливости (поступки, считающиеся нарушающими эти правила, перечислены особо и включают преследование, обнародование личных сведений о ком-то без его согласия, оскорбления, угрозы, клевету, а также нарушение авторских прав и коммерческой тайны).
- Не писать ничего такого, чего не сказали бы собеседнику лично.
- В конфликтных ситуациях перед тем, как отвечать публично, сначала связываться с собеседником приватно и прояснять позицию.

[14] http://bloging.wikia.com/wiki/blogger's_Code_of_Conduct

- Принимать меры против необоснованных нападок на других.
- Не допускать анонимных комментариев (или даже более жестко - не принимать псевдонимов).
- Игнорировать провокаторов (в Сети они получили название тролли - trolls).
- Требовать исполнения правил, в том числе с применением силы и власти.
- Не раскрывать источники (кроме как по решению суда).
- Быть разумным в удалении комментариев (даже если они противоречат убеждениям).
- Не причинять вреда.

Вероятнее всего, черновик не останется черновиком надолго, так как сообщество с интересом отнеслось к идее редактирования кодекса в Wikipedia и постоянно изменяет текущую версию, подчас кардинальным образом меняя смысл некоторых пунктов. Однако подобный свод правил, несмотря на то, что он появился относительно недавно, уже приобрел как ярых сторонников, так и противников. Первые считают, что создание подобных кодексов позволит сделать Сеть более цивилизованным местом, а противники свода правил видят в нем проявление цензуры. Однако большинство правил восходит к простым общечеловеческим нормам поведения. Многие пользователи Сети и без данного кодекса считают, что необходимо придерживаться в Интернете тех же правил поведения, которые мы соблюдаем в реальной жизни: не надо говорить человеку в Интернете того, чего не сможешь повторить, глядя ему в глаза; нужно уважать частную жизнь пользователей, нехорошо общаться с анонимами; следует держать себя в руках во время Интернет-ругани, и, наконец, лучше игнорировать сообщения провокаторов - не получая отклика, они потеряют к вам всякий интерес.

О'Рейли и Уэйлс заявили, что возможно, будет создан не один, а три различных кодекса поведения для блоггеров, которые будут отличаться друг от друга по отдельным пунктам, вызвавшим наибольшие споры. Например, в

одном из них анонимные комментарии запрещаться не будут, в другом - будут, а в третьем - будут запрещаться высказывания даже тех лиц, которые скрываются за псевдонимами (пусть даже известными). В одном из них можно будет скрывать источники информации, и публиковать слухи, а в другом при публикации срочных новостей обязательно нужно будет давать ссылки на первоисточники. В зависимости от того, каким из этих трех сводов будет руководствоваться тот или иной блоггер, он будет размещать на страницах своего дневника соответствующий баннер с указанием кодекса, по правилам которого ведется общение.

По-видимому, блогосфера и соцсети будет жить и развиваться и безо всяких правил. Правила общения создаются самим сообществом, а О'Рейли просто попытался их сформулировать для тех, кто еще не определился с манерой поведения в Интернете.

Правила поведения в Интернете от Microsoft

Компания Microsoft , в свою очередь, не осталась в стороне от обсуждения вопроса поведения в Интернете и опубликовала собственные "Правила" в виде советов родителям. Причем по приведенному образцу предлагается написать собственный семейный кодекс поведения, которому согласятся следовать все члены семьи. Правила использования Интернета можно написать для каждого ребенка в семье с учетом его возраста. На соответствующей странице сайта компании (http://www.microsoft.com/rus/athome/security/children/famwebrules.mspx) предлагается образец такого соглашения.

Соглашение о кодексе поведения в Интернете

Я обязуюсь:

- обращаться к моим родителям, чтобы узнать правила пользования Интернетом: куда мне можно заходить, что можно делать и как долго позволяется находиться в Интернете (_____ минут или _____ часов);
- никогда не выдавать без разрешения родителей личную информацию: домашний адрес, номер телефона, рабочий адрес или номер телефона

родителей, номера кредитных карточек или название и расположение моей школы;

- всегда немедленно сообщать родителям, если я увижу или получу в Интернете что-либо тревожащее меня или угрожающее мне: включая сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в Интернете;
- никогда не соглашаться лично встретиться с человеком, с которым я познакомился в Интернете, без разрешения родителей;
- никогда не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет или обычной почтой;
- никогда никому, кроме своих родителей, не выдавать пароли Интернета (даже лучшим друзьям);
- вести себя в Интернете правильно и не делать ничего, что может обидеть или разозлить других людей или может противоречить закону;
- никогда не загружать, не устанавливать и не копировать ничего с дисков или из Интернета без должного разрешения;
- никогда не делать без разрешения родителей в Интернете ничего, требующего платы;
- сообщить моим родителям мое регистрационное имя в Интернете и имена в чате, перечисленные ниже:

Конечно, российская ментальность вряд ли позволит родителям даже предлагать своим детям подписание такого соглашения, но в целом приведенные правила представляются вполне разумными.

6. О себе – только имя

Совет: Никогда не высылайте сетевым друзьям и собеседникам, особенно анонимным, тем, с кем вы не встречались и общались в реальной жизни, своих личных данных, домашнего адреса, копий документов и пластиковых карт, ваших приватных фотографий и изображений, фотографий с другими лицами.

Соображения пользователей соцсетей по этому поводу можно резюмировать следующим ироничным списком:

1. Если вы хотите хорошо продать ваш товар, просто изобразите на рекламе кота.
2. Если вы хотите познакомиться с девушкой в соцсетях, просто поставьте «лайк» под ее фото.
3. Если ваш ребенок мало времени проводит в соцсетях, значит у вас в друзьях его ненастоящий профайл.
4. Если в ресторанах и клубах тебя угощают кофе и коктейлями, значит ты – активный пользователь Foursquare.
5. Прежде, чем ставить лайк или комментировать фотографии симпатичных девушек, помните: вас могут обвинить в измене.
6. Вы можете быть тем, кем захотите. Главное подобрать правильную аватарку и информацию в профиле.
7. Если у вас есть тёмная сторона личности, лучше скрыть её за отдельным аккаунтом.
8. Чтобы быть интересным собеседником, перед свиданием с девушкой прочитайте, о чем пишут ВКонтакте
9. Процитируй у себя на стене Стива Джобса и люди не будут думать, что ты неудачник.
10. Если лето выдалось унылым и у вас нет фотографий с моря, пости демотиваторы и статьи о политике.

11. Если у вас нет денег, чтобы купить девушке букет цветов и сводить ее в ресторан, вы можете завоевать ее, поставив статус «Влюблен в…»

12. Не думайте, что кто-то вспомнит о вашем дне рождения, если вы не указали его ВКонтакте.

По фотографии из Facebook можно идентифицировать любого человека, встреченного на улице. Более того, о нем можно получить всю информацию, опубликованную в Интернете, доказали авторы исследования «Лица Facebook: Частная жизнь в эпоху дополненной реальности» («Faces of Facebook: Privacy in the Age of Augmented Reality»)[15].

У социальной сети Facebook уже возникали проблемы из-за технологии распознавания лиц на фотографиях, которая позволяет автоматически отмечать пользователей в альбомах друзей, напоминает техноблог Mashable. В июне текущего года крупнейшая мировая соцсеть начала внедрять функцию Tag Suggestions, и вокруг нее вспыхнули бурные дебаты. Некоторые пользователи и правозащитники восприняли использование этой технологии как попытку вторжения в личное пространство и нарушение права на неприкосновенность частной жизни.

Тогда возможность случайного «отмечания» любого человека, попавшего в кадр, настолько взбудоражила общественность, что рассмотрением данного вопроса занялась Еврокомиссия.

Теперь же возникла куда более серьезная тема для размышлений: любой человек, имеющий профиль в Facebook, фактически находится в базе данных, которой может воспользоваться кто угодно.

Пользователь соцсети может быть идентифицирован прямо на улице — достаточно лишь сфотографировать его на камеру мобильного телефона и воспользоваться специальной программой распознавания. Об этом рассказали на конференции по компьютерной безопасности Black Hat в Лас-Вегасе

[15] http://vkurse.ru/article/4855305/

создатели приложения «дополненной реальности» для мобильных устройств из Университета Карнеги-Меллона.

Исследователи Алессандро Аквисти (Alessandro Acquisti), Ральф Гросс (Ralph Gross) и Фред Стутзман (Fred Stutzman) собрали базу из 25 тысяч фотографий студентов-пользователей Facebook, а затем предложили желающим «заглянуть в веб-камеру», расположенную в одном из университетских кампусов. В результате были опознаны личности 31% студентов. На анализ фотографий у программы в среднем уходило около 3 секунд.

Затем был проведен еще один эксперимент, в ходе которого 278 тысяч фотографий из Facebook сравнивались с 6 тысячами фотографий анонимных пользователей сайтов знакомств. В итоге был опознан каждый десятый.

По мнению авторов исследования, буквально через несколько лет программы визуального поиска могут стать столь же часто используемыми, как сегодняшние текстовые поисковые системы.

Это «ужасная угроза для частной жизни», заявил профессор в области информационных технологий и государственной политики Алессандро Аквисти. Широкое распространение технологий, позволяющих по фотографии находить реальные имена и информацию в огромных базах социальных сетей, подорвет само понятие анонимности. С другой стороны, подобные технологии очень пригодятся правоохранительным органам для опознания и поимки преступников. Кстати, исследования Университета Карнеги-Меллона частично финансируются армией США, отмечает ресурс Cnet.

Источником данных о пользователе не обязательно должен быть Facebook — точно так же можно воспользоваться открытыми данными из любой соцсети, будь то LinkedIn, Google+ или «Одноклассники». Исследователи остановились именно на Facebook лишь потому, что сегодня это самая большая соцсеть в мире.

Пока технология несовершенна, признают авторы исследования. Для того, чтобы программа распознала человека, его нужно снять определенным образом, в фас, а не под углом. Однако развитие технологий идет такими

темпами, что не за горами более продвинутые средства. «То, для чего сегодня требуются мобильные устройства, завтра можно будет осуществить совсем незаметно. Незнакомец сможет прочитать вашу последнюю запись в Twitter, просто взглянув на вас», — предрекает Аквисти.

По данным on-line опроса, проведенного информационным каналом Subscribe.ru[16], среди 5500 пользователей, представляющих активную (месячную) российскую интернет-аудиторию, последняя практически полностью вовлечена в социальные сети. Около 13% пользователей зарегистрированы хотя бы в одной соцсети, 22% — в двух социальных сетях. Каждый четвертый (25%) пользователь зарегистрирован в трех, а каждый третий (33%) — более чем в трех социальных сетях. При этом около 59% среди пользователей социальных сетей ежедневно посещают хотя бы одну Сеть из числа тех, где они зарегистрированы; около четверти (25%) делают это несколько раз в неделю, а 15% — не чаще одного раза в неделю. И только 6% опрошенных пользователей не зарегистрированы ни в одной из социальных сетей.

Что же о себе рассказывают пользователи социальных сетей? 80% сообщают такие сведения, как имя и фамилия, только пол указывают 78%, дату рождения пишут 74%, лишь возраст — 60%, образование — 66%. Указанные пользователи не переживают, что использование данных другими людьми (в том числе, несанкционированное) может причинить им какой-либо вред. При этом 52% пользователей социальных сетей для сохранения конфиденциальности лишь ограничивают права других пользователей в возможности просмотра их личной информации.

Стоит отметить, что данная статистика касается российских пользователей. В Европе ситуация иная, и об этом мы не раз писали и говорили на конференциях. И связано это с таким банальным, казалось бы, фактором, как осознание потенциальной опасности. Кроме того, в европейских странах вопросы защиты информации и персональных данных в Интернете — тема не

[16] http://www.privacy-info.ru/events-pd/2012/05/08/Social-networks-possible-control-working-personal-data.html

новая, и уже со школы детей знакомят с правилами поведения в Сети и объясняют опасность излишней открытости.

Но вернемся к нашей стране. Бум социальных сетей уже миновал, россияне поняли, что своих социальных сетей недостаточно, и потянулись к зарубежным сервисам. Facebook, Goggle+, Netlog казались заманчивыми до тех пор, пока пользователи не почувствовали, что ситуация становится неконтролируемой: персональные данные, фотографии, иная личная и конфиденциальная информация, однажды загруженная в социальной сети, «гуляет» по Интернету и ее невозможно удалить. К сожалению, в Федеральном законе Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и других подзаконных актах такие моменты, как защита персональных данных в Интернете, четко и однозначно прописаны не были. Потому первые случаи «утечки» личной информации застали пользователей социальных сетей врасплох, более того — люди понятия не имели, куда обращаться за помощью, особенно, если произошедшая утечка причинила моральный или даже материальный ущерб. Возникает вопрос - является ли владелец социальной сети оператором персональных данных?

7. Подробности – ключи для воров

Многие подробности нашей повседневной жизни, которые кажутся нам незначительными, для бандитов могут стать достаточной информацией для планирования преступления. Где вы часто гуляете? Где вы прописаны? По какой улице вы ходите домой? В каком районе расположена школа вашего ребёнка? Куда и когда вы собираетесь поехать на отдых? В каком банке вы обслуживаетесь? Сколько у вас детей, их имена? Имена родителей? Марка и модель вашего автомобиля? По этим данным преступник может составить карту вашей личности и воспользоваться ими в своих целях.

Подробности личной жизни, размещенные в социальной сети – и есть та точка, где виртуальное и может вторгнуться в нашу реальную жизнь.

Часто сетевые записи - это тот самый ключ от квартиры, где деньги лежат.

Один из успешных бизнесменов разместил в социальной сети фоторепортаж о своем отдыхе в одной из экзотических стран. Сразу после этого он получил предложения дружбы от симпатичной девушки, которая очень подробно интересовалась подробностями путешествия, в том числе и туристическим агентством, которое бронировало тур.

В ходе общения турист заметил, что забронировал тур с бонусной карты и заработал тем самым на бесплатный авиабилет. Этих подробностей, а также внимательно прочитанного блога, в котором после дружбы стали доступны большинство записей, гражданину N, выдававшего себя за любопытную девушку хватило, чтобы определить номер карты и совершить по ней несколько операций, прежде чем владелец успел ее заблокировать.

Журнал The Times[17] опубликовал статью, в которой призывает читателей продуманно относиться к поведению в интернете: красочный рассказ о бурных выходных может стоить карьеры. А работодателям и рекрутерам есть где развернуться. По данным Badenoch & Clark, международной консалтинговой

компании, практически две трети (62%) британских менеджеров зарегистрированы в Facebook, MySpace или других социальных сетях. Каждый пятый британский работодатель признался, что хотя бы раз использовал подобные сайты для поиска информации о кандидатах и изучал, как те преподносят себя. Почти две трети сообщили, что обнаруженная информация повлияла на их решение о приеме на работу. По словам четверти руководителей, они изменили свое решение и предпочли не брать человека на работу из-за найденных в сети данных.

«Мы не используем интернет, предпочитаем ориентироваться при принятии решения на результаты интервью и рекомендации», - говорит Ольга Филатова, начальник департамента по кадровой политике компании «МегаФон». «Социальные сети мы используем исключительно для поиска интересных для компании людей, но ни в коем случае не для проверки, - утверждает Анастасия Пречистенская, директор по персоналу Strategy Partners. - Мне кажется, люди уже давно осознали публичность таких ресурсов и сами не выкладывают туда ничего компрометирующего».

Несколько менее категоричны представители рекрутинговых компаний. По мнению Эльвиры Смагиной и Анастасии Дементьевой, консультантов компании «Империя кадров», такие ресурсы, как «Одноклассники» и «В контакте», активно используются рекрутерами: «Они дают возможность получить более полную информацию о кандидатах. Однако нужно помнить, что у каждого есть свои интересы и порой они бывают специфическими. Главное, чтобы впоследствии это не влияло на репутацию компании». «Информация в социальных сетях может использоваться лишь как дополнительный ресурс, когда уже все имеющиеся у эксперта инструменты исчерпаны, - считает Нина Карелина, управляющий партнер КГ ИМИКОР. - Более продуктивно и, безусловно, этично использовать технологию прямого поиска».

Примеры вреда, нанесенного карьере активным присутствием в социальных сетях, нам пока не известны. Но вот о том, как неосторожные

[17] http://www.keep-intouch.ru/analytics/work.htm

высказывания лишили хорошего профессионала новой работы, рассказал RB.ru Руслан Тотров, руководитель команды компании Antal International: «Мы искали директора по маркетингу. Все перспективные кандидаты были людьми публичными, были на виду. Особенно интересной показалась кандидатура достаточно известного в профессиональных кругах человека из солидной компании, полностью соответствовавшего требованиям работодателя. Однако весьма интересные детали "всплыли", когда решили задействовать открытые источники и составить небольшое информационное досье на кандидата. Выяснилось, что претендент любит делать резкие заявления для СМИ относительно деятельности конкурентов, порой переходя на личности. Эта его особенность даже была предметом детального обсуждения на одном из профессиональных блогов. От рассмотрения этой кандидатуры мы отказались».

Призывают к осторожности и британские консультанты. «Большинство людей присутствуют онлайн во множестве ипостасей, и не обязательно все они показывают человека с лучшей стороны, - считает Энди Пауэлл, директор Badenoch & Clark. - Большинство работодателей принимает в расчет "сетевую репутацию", так что проявить немного осторожности - правильное решение».

Совет. При пользовании различного рода блогами и дневниками старайтесь по возможности не упоминать критичные и конфиденциальные подробности своей жизни и других лиц, включая публичных персон.

8. Самая невосполнимая потеря

Как это ни странно, но наибольший вред соцсети причиняют нам, похищая наше время. Эти потери значительно превосходят все возможные утечки информации или финансов, вероятные в виртуальном мире.

Олег пельмени бросил в воду,
Приправил их, прибавил газ...
Зашел вконтакт, проверить почту...
Вот так сгорело пять квартир!

В настоящее время, на социальные сети приходится 18% времени, проведенного в интернете[18].

С 2006 года время, потраченное на сайты социальных сетей, увеличилось более чем в два раза, с 2,7 часов до 6,9 часов в месяц. Так же и увеличивается число пользователей социальных сетей.

Средний пользователь Facebook проводит на сайте примерно семь часов каждый месяц. Средний посетитель в Twitter, LinkedIn и Google+ тратит меньше, чем полчаса на сайт в месяц.

По результатам последних статистических исследований[19], граждане Российской Федерации большое количество времени проводят в различных социальных сетях – как зарубежных, так и отечественных. В среднем это бело десяти часов в месяц.

Глобальное исследование активности жителей из разных стран по отношению к социальным сетям, проведенное аналитическим бюро comScore показало, что на втором месте в мире по занятости в пространстве социальных сетей сегодня занимают россияне. В среднем российский пользователь интернет проводит в социальных сетях 10,3 часа в месяц.

[18] http://svetlanabekshansocial.com/B4.html/

[19] http://www.internovosti.ru/text/?id=51926

Только граждане и жители Израиля могут соперничать с россиянами в том, сколько времени проводят в общении на страничках социальных сетей. Жители Израиля могут похвастаться в этом совершенным мировым лидерством – они в соцсетях находятся примерно 10,7 часа ежемесячно. За Россией по количеству времени, проводимому в соцсетях следуют Аргентина, Филиппины, Турция, Венесуэла и Колумбия. В среднем их показатель – это от восьми с половиной до семи часов ежемесячно. США и Англия проводят в соцсетях еще меньше.

Каждый участник социальной сети Google+ в январе провел там около 180 секунд. Информацию об этом дает The Wall Street Journal[20]. Согласно этим данным, в них не было включено время, проведенное в социальной сети при помощи мобильного телефона.

Компания Google подчеркнула, что их статистические данные разнятся с показателями comScore, но конкретных данных они не привели.

Все познается в сравнении. Как сообщает comScore, в первый месяц нового года, участник социальной сети Facebook провел там около семи часов, а Twitter - около двадцати минут.

По эти показателям Google+ обогнали MySpace - 8 минут и Linkedin -17 минут.

Социальная сеть Google+ появилась летом прошлого года, а уже осенью можно было стать полноправным ее участником. В летнее время, по приглашениям стать участником, Google+ опередил Facebook и Twitter. Как сообщает comScore, за несколько недель в Google+ стало четверть миллиона участников. А в первые дни после того, как приглашение отменили, на страничку Google стало заходить на 1269 % людей больше.

В первый месяц нового года социальная сеть Google отметила, что число зарегистрировавшихся в Google+ составило более 90 миллионов людей. 60% от числа этих людей посещают свою страничку каждый день, а 80% - раз в неделю.

[20] http://freezly.ru/forum/1-316

Совет. Ограничьте время своего пребывания в соцсети, помните, что реальный мир богаче и интересней.

9. Социальные сети и работа

По возможности не пользуйтесь соцетями на работе и службе, если это нужно по каким-либо причинам, выделите для этого отдельный компьютер

Если Вы руководитель - не запрещайте пользоваться соцсетями, иначе работники будут изыскивать время и возможности в ущерб служебным обязанностям, при этом разумно ограничьте время и поддерживайте меры безопасности.

Компаниям не следует запрещать сотрудникам пользоваться на работе социальными сетями типа Facebook - к такому выводу пришли специалисты британского исследовательского центра Demos[21]. По их мнению, попытки запрета могут в конечном счете повредить самим работодателям, так как ограничивают возможности сотрудников для общения. Авторы исследования считают, что социальные сети помогают людям выстраивать отношения с коллегами внутри организации. Исследователи выявили, что различные компании все шире используют социальные сети для обмена документами и сотрудничества в разработке новых идей. Если более ориентированные на работу сети типа LinkedIn или специально сделанные по заказу руководства программы внутренней связи используются исключительно в рабочих целях, то в рабочем графике можно найти время и для сетей типа Facebook, Bebo и MySpace, считает специалист Demos и автор исследования Питер Брэдуэлл. "Они - неотъемлемая часть человеческого общения, и людям нравится его интуитивный характер", - говорит он. "Запрет Facebook и других подобных сетей вступает в противоречие с естественной потребностью людей в общении. Часто благодаря таким сетям между сослуживцами возникают дружеские отношения", - добавляет Брэдуэлл. Он также считает, что использование технологий для укрепления связей между бывшими коллегами и потенциальными клиентами повышает производительность, новаторство и

создает демократичную рабочую среду. "Предоставление сотрудникам большей свободы и гибкости может показаться контр-продуктивным, но на самом деле позволяет компаниям поддерживать стабильность", - говорит Брэдуэлл. Популярность социальных сетей свидетельствует о наличии у людей желания общаться друг с другом, говорит Марк Таррелл, глава фирмы Imaginatik, которая специализируется на создании по заказу компаний специальных внутренних коммуникативных сетей. "Возможность увидеть фото коллеги или узнать, чем он занимается, может оказаться чрезвычайно полезной для бизнеса, особенно если в фирме работают тысячи людей", - говорит Таррелл. В то же время он признает, что использование коммуникативных сетей должно "подчиняться интересам дела". Как рассказал Таррел, клиенты его фирмы через такие программы знакомят сотрудников с проблемами, которые стоят перед ними, и выносят их на всеобщее обсуждение. "Через несколько дней внутри компании выявляется достаточное количество людей, которые способны предложить тот или иной выход из проблемы", - говорит он. Молодые сотрудники, выросшие в эпоху интернета, мобильных телефонов и социальных сетей хотят, чтобы работодатели гибче приспосабливались к новым технологиям. "Ключевой вопрос состоит в том, каким образом привлечь к себе как можно больше способной молодежи", - говорит Таррелл. "Фирмы должны предоставлять своим сотрудникам физическое и виртуальное пространство для роста и развития своих идей". В то же время авторы доклада говорят, что необходимо выработать определенные критерии правильного использования социальных сетей. Руководство без смущения должно ставить на вид тем сотрудникам, которые "неразумно много" времени проводят в сетях с нерабочими целями. Заказавшая исследования компания мобильной телефонной связи Orange сама в настоящее время создает собственную внутреннюю коммуникативную связь для сотрудников. "Роль и значение социальных сетей быстро растет из-за развития новых технологий, которые позволяют людям связываться друг с другом в професиональной и частной

[21] http://www.keep-intouch.ru/analytics/work.htm

жизни", - говорит представитель Orange Роберт Эйнгер. "Но в то же время компании должны осознавать существующие проблемы и устанавливать правила, которые будут развивать, а не сдерживать благотворное воздействие сетей".

10. Молчать вредно

Часто причиной многих сетевых преступлений становится излишняя пассивность и терпеливость граждан. Потеря небольшой суммы, моральный удар часто сходят бандитам или хулиганам с рук. И так может длиться годами. А между тем больше половины преступлений можно предотвратить простой своевременной жалобой администратору.

Совет. Не стесняйтесь жаловаться на некорректное поведение пользователей-троллей администрации соцсетей, другим пользователям и уполномоченным контролирующим органам.

Пожалуй, не много найдется людей, которых ни разу не оскорбили на форумах, в чатах или в различных социальных сетях.

Хаму кажется, что в Интернете он анонимен, и под виртуальной маской можно писать все что угодно. Можно безбоязненно обидеть человека и не надо будет опасаться, что кто-либо узнает имя обидчика или каким-либо образом заставит ответить за свои слова.

Хаму кажется, что в Интернете он анонимен, и под виртуальной маской можно писать все что угодно. Можно безбоязненно обидеть человека и не надо опасаться, что кто-либо узнает имя обидчика или каким-либо образом заставит ответить за свои слова.

К сожалению, в большой степени это мнение оправдано. Мало кто решается обратиться в суд и защитить себя, свою репутацию и свое достоинство. В России почти нет прецедентов по разрешению споров об оскорблении в Интернете. У кого-то нет денег, кому-то лень, кто-то боится прослыть сутягой. А клеветы и оскорблений с каждым днем становится все больше. Что же делать, как защитить себя от виртуального произвола?

Итак, давайте рассмотрим, какие есть рычаги воздействия на хамов, и как можно защитить себя от оскорблений в Интернете?[22]

[22] http://www.kreuzmarine.com/index.php?option=com_content&task=view&id=52&Itemid=44

Во-первых, каждому пользователю Интернета, конечно же, надо знать свои права, отраженные в законодательных актах Российской Федерации.

1. Конституция, статья 21 гласит:

Достоинство личности охраняется государством. Ничто не может быть основанием для его умаления.

2. Уголовный Кодекс, статья 129 гласит:

Клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, наказывается:

- штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года,
- - либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов,
- - либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев.

3. Уголовный Кодекс, статья 130 гласит:

Оскорбление, содержащееся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, наказывается:

- штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев,
- - либо обязательными работами на срок до ста восьмидесяти часов,
- - либо исправительными работами на срок до одного года.

4. Гражданский Кодекс, статья 152 гласит:

Гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности.

Что можно требовать в Гражданском суде:

1. Гражданин вправе требовать возмещения убытков и морального вреда, причиненных распространением сведений, порочащих честь, достоинство или деловую репутацию гражданина.

2. Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, распространены в СМИ, они должны быть опровергнуты в тех же средствах массовой информации.

3. Гражданин, в отношении которого средствами массовой информации опубликованы сведения, ущемляющие его права или охраняемые законом интересы, имеет право на опубликование своего ответа в тех же СМИ.

Тем не менее надо помнить, что не все сайты являются СМИ. Средство массовой информации – это периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации, зарегистрированное в установленном законом порядке.

Соответственно, опровержения информации и опубликования своего ответа можно требовать только у СМИ. Возмещения убытков можно требовать у всех тех, кто распространял сведения, порочащие честь, достоинство или деловую репутацию гражданина.

Какие действия надо производить в случае оскорбления в Интернете.

Если вы хотите удалить оскорбительную информацию с Интернет-ресурса, вам нужно направить бумажное письмо (претензию) владельцу сайта. Если на сайте адрес не указан, тогда можно направить письмо по электронной почте. В данном письме нужно изложить ситуацию и потребовать убрать всю оскорбительную информацию, сославшись на указанные выше статьи.

Если же удаления информации вам недостаточно, ваши действия должны быть таковы:

1. Написать бумажную претензию владельцу сайта или (и) доменного имени.

Имя физического лица (или фирменное наименование организации), администратора домена, можно узнать в базе данных РосНИИРОС, воспользовавшись WhoIs-сервисом.

В данной справке указан адрес гражданина или место нахождения организации, адреса DNS-серверов, и иная полезная для обращения в суд и нахождения ответчика информация.

Информация о владельце домена, содержащаяся в закрытой базе данных РосНИИРОС, может быть предоставлена по письменному запросу суда, правоохранительных органов или адвокатскому запросу.

2. Направить бумажное письмо (претензию) провайдеру сайта, на котором размещена оскорбительная информация.

Провайдера также можно узнать в базе данных РосНИИРОС, воспользовавшись WhoIs-сервисом. Заявление надо писать на имя руководителя компании. Письмо лучше направлять заказным сообщением, с уведомлением. Уведомление о получении ими письма впоследствии необходимо будет предъявить в суде.

3. Написать заявление в правоохранительные органы.

Статьи 129 и 130 Уголовного Кодекса РФ (клевета и оскорбление) расследуются дознавателями органов внутренних дел. Поэтому заявление лучше писать и нести (либо отправлять по почте) в милицию – местное УВД. Подавать заявление можно по вашему месту жительства или временного пребывания.

В случае отказа милиции в возбуждении дела этот отказ следует обжаловать прокурору также по вашему месту жительства. Правоохранительные органы должны повести расследование и установить гражданина, скрывающегося за ником человека, оскорбившего вас в сети. Если же имя гражданина вам известно, то это стоит указать в заявлении. Затем, возможно, будет проведено судебное следствие.

4. Подать в суд гражданский иск против владельца сайта, либо лица, опубликовавшего оскорбительную информацию.

Для того, чтобы дело решалось в суде, вам надо будет собрать доказательную базу – то есть, распечатать и заверить у нотариуса все веб-страницы, на которых размещены оскорбительные отзывы. К сожалению, не все нотариусы заверяют информацию, размещенную в Интернете, поэтому, таких специалистов надо искать. Наверняка, они найдутся в любом более-менее крупном городе.

Иногда для того, чтобы определить, является ли высказывание «порочащим честь, достоинство или деловую репутацию гражданина», нужно произвести соответствующую лингвистическую экспертизу. Проводят ее различные Центры Судебных Экспертиз. Эксперты смогут высказать официальное мнение о том, является ли Интернет-высказывание утверждением, предположением или оценочным суждением. Также, можно будет определить характер содержащихся в высказывании сведений (сведения о фактах или событиях или иные суждения), понять, относятся ли высказывания именно к вам. Данная экспертиза является платной.

Если вы намерены защищаться в суде, вам, конечно же, понадобится адвокат. Он поможет составить грамотное исковое заявление, подать его в суд, оплатить госпошлину, составить необходимые ходатайства и надлежащим образом защитить ваши интересы в суде.

Достаточно часто бывает необходимо выяснить информацию о конкретном сайте, связанном с доменным именем. Необходимость этого может быть продиктована целесообразностью получения дополнительной информации о контрагентах или партнерах.

Для решения этой задачи используется ресурс www.nic.ru.

На стартовой странице этого сайта есть вкладка «Whois», которая позволяет получить информацию о владельце домена. Зададим для получения информации домен Центрального банка РФ и получим следующий результат:

Информация о домене CBR.RU

Домен занят.

по данным WHOIS.NIC.RU:

% By submitting a query to RU-CENTER's Whois Service

% you agree to abide by the following terms of use:

% http://www.nic.ru/about/servpol.html (in Russian)

% http://www.nic.ru/about/en/servpol.html (in English).

domain: CBR.RU

nserver: ns1.cbr.ru.

nserver: ns2.cbr.ru.

nserver: ns3.cbr.ru.

state: REGISTERED, DELEGATED

phone: +7 495 7539295

phone: +7 495 7539221

fax-no: +7 495 7539249

e-mail: postmaster@cbr.ru

org: Center of information technologies of the Bank of Russia

registrar: RU-CENTER-REG-RIPN

created: 2004.11.19

paid-till: 2011.12.01

source: RU-CENTER

Last updated on 2011.07.25 01:44:07 MSK/MSD

Описание полей в ответах WHOIS-сервиса о доменах

по данным WHOIS.TCINET.RU:

% By submitting a query to RIPN's Whois Service

% you agree to abide by the following terms of use:

% http://www.ripn.net/about/servpol.html#3.2 (in Russian)

% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

domain: CBR.RU

nserver: ns1.cbr.ru. 212.40.192.35

nserver: ns2.cbr.ru. 212.40.193.252

nserver: ns3.cbr.ru. 212.40.192.37

state: REGISTERED, DELEGATED, VERIFIED

org: Center of information technologies of the Bank of Russia

phone: +7 495 7539295

phone: +7 495 7539221

fax-no: +7 495 7539249

e-mail: postmaster@cbr.ru

registrar: RU-CENTER-REG-RIPN

created: 1996.11.10

paid-till: 2011.12.01

source: TCI

Легко видеть, что полученная информация исчерпывающе описывает свойства домена, указывает контактные телефоны и почту для связи с владельцами домена, а также полное наименование владеющей доменом организации.

Несколько более сложной является ситуация, когда часть данных закрыта или домен принадлежит физическому лицу. В этом случает необходимо выполнить ряд уточняющих запросов.

Рассмотрим практический пример.

Торговая марка «Мисс Беллиданс» на территории РФ принадлежит юридической фирме «Малахов и партнеры». В то же время в доменной зоне RU проводится конкурс «Мисс Беллиданс», информация о котором размещена на сайте missbellydance.ru.

Результат выполнения запроса:

Информация о домене MISSBELLYDANCE.RU

Домен занят.

по данным WHOIS.NIC.RU:

% By submitting a query to RU-CENTER's Whois Service

% you agree to abide by the following terms of use:

% http://www.nic.ru/about/servpol.html (in Russian)

% http://www.nic.ru/about/en/servpol.html (in English).

domain: MISSBELLYDANCE.RU

nserver: ns1.hc.ru

nserver: ns2.hc.ru

state: REGISTERED, DELEGATED

person: Private person

phone: +7 495 0000000

e-mail: missbust@mail.ru

registrar: RU-CENTER-REG-RIPN

created: 2006.07.30

paid-till: 2011.07.30

source: RU-CENTER

Как видно из результатов поиска владелец домена пожелал остаться неизвестным, но в качестве контактной информации присутствует электронная почта. Имя электронной почты наводит на мысль о связи данного конкурса с конкурсом «Мисс Бюст». Кроме того, в номере телефона указан код Москвы. Расширенный поиск по запросам «Мисс Бюст Москва» и «Мисс Беллиданс Москва» приводит к владелице сайтов missbust.ru, beledi.ru, baladi.ru, missbellydance.ru и miss-dance.ru Савельевой Галине.

Достаточно информативным является установление членства акционеров в различных предприятиях.

Для этого можно использовать следующие конструкции поиска

«наименование предприятия акционеры» или

«наименование предприятия список акционеров»

Так, например, поиск в Yandex по запросу

домодедово список акционеров

дает следующие результаты:

Счетная палата нашла владельца «Домодедово» — кипрскую компанию «Асьенда инвестментс лимитед». 20 апреля Генпрокуратура признала, что ей эта задача не под силу и предложила ограничить доступ иностранцев к стратегическим объектам транспорта.

Счетная палата РФ сумела выявить истинного владельца «Домодедово». Им является кипрская компания «Асьенда инвестментс лимитед», под управлением которой находятся 322 объекта недвижимости и инфраструктуры аэропорта. Факт собственности был установлен по результатам проверки, сообщает СП 3 мая.

А также

Единственным владельцем DME Limited, холдинговой компании «Домодедово», является Дмитрий Каменщик (№86 списка богатейших бизнесменов России, состояние - $1,1 млрд). Об этом сообщает агентство «Интерфакс». Ранее предполагалось, что совладельцем аэропорта также является Валерий Коган.

«На данный момент Дмитрий Каменщик является конечным бенефициаром 100% акций компании», - говорится в сообщении DME Limited на Лондонской фондовой бирже (LSE). Компания в среду, 18 мая, официально объявила о своем намерении провести IPO на LSE.

В ряде случаев необходимо бывает выяснить контактную информацию конкретных физических лиц. Для этой цели целесообразно использовать общедоступные телефонные и адресные справочники. В частности, весьма информативным является следующий ресурс http://www.nomer.org/

На этом ресурсе возможен достаточно простой поиск физических лиц как по известному телефону, так и по элементам фамилии, имени и отчества. Для поиска данных по известному адресу возможно использовать ресурс http://ibaza.org/.

Кроме того, используя поиск конструкций «телефонный справочник» или «телефонный справочник москвы», можно найти ссылку как на указанные выше ресурсы, так и на другие достаточно интересные ресурсы, включая http://www.spr.ru/, содержащий информацию о предприятиях Москвы и области.

При работе с персональными данными, полученными из открытых источников необходимо помнить о том, что на территории РФ действует закон о персональных данных - Федеральный закон РФ 27.07.2006 г. № 152-ФЗ "О персональных данных".

11. Дети и сети

Дети не имеют многих социальных навыков, иммунитета ко многим опасностям и просто жизненного опыта. Поэтому там, где взрослый человек даже не заметит опасности, ребёнок может попасться в смертельную ловушку.

На самом деле весьма важный вопрос, который часто остается за границей обсуждения и восприятия - как современные медиа влияют на мозг человека и детей в частности[23]? Каждая личность уникальна, с самого детства мы абсолютно разные. Мозг человека уникален и на всей планете не найдется двух одинаковых. Информационная и социальная среда, в которой растет человек, очень важна, это все то, что будет отпечатываться, все то, что будет формировать сознание и картинку мира.

Совсем недавно был проведен эксперимент с пианино. Три группы испытуемых, первая группа просто смотрела на рояль, вторая — учила гаммы, третья группа представляла, что играет на рояле.

Мозговая активность третьей группы были почти такие же, как у второй, т.е. у тех, кто непосредственно играл на пианино. Из чего следует вывод – даже просто воображаемое действие влияет на развитие и структуру мозга.

Чем опасны социальные сети для детей? Одна из опасностей – снижение эмпатии, неумение сопереживать.

Дети, выросшие в социальных сетях, постепенно утрачивают навыки межличностного общения — они не умеют краснеть, прикасаться друг к другу, искренне реагировать на действия других детей, а главное - получать немедленный ответ от собеседника и вести диалог, поскольку комментарии и общение он-лайн – все же имитация реального эмоционального диалога.

При восприятии другого человека впечатление о нем складывается на 70% из невербальной информации, именно так работает человеческий мозг. А общаясь в соцсетях, дети как бы замыкаются в двумерном пространстве.

[23] http://rastemvrossii.ru/obrazovanie-v-rossii/shkola/spetsialisti/deti-i-sotsialnye-seti.html

Масштаб негативных воздействий социальных сетей, безусловно, зависит от конкретного человека, но дети практически беззащитны перед таким воздействием. Ребенку необходимо показывать положительный опыт в реальном мире и побуждать его использовать виртуальный мир разумно,. В противном случае, у детей будут развиваться синдромы дефицита внимания и гиперактивности.

Интересно проследить, как развивалось общение людей в интернете. В 1999 году люди писали в Livejournal, что у них есть кот, в 2004-м — выкладывали фото и видео этого кота, в 2010-м они могут писать в твиттер раз в час о том, что их кот чихнул.

Появилась возможность и люди начинали говорить друг другу о том, что никому и не нужно знать. Пользователи соцсетей как маленькие дети. Они как будто говорят маме: «Посмотри, я уже умею одевать колготки». Более того, ждут обратной реакции, оценки, т.е. подтверждения собственного существования на Земле.

Еще одна опасность соцсетей для детей в том, что человек не умеет оценивать риски. Почти все виртуальные действия не имеют необратимых последствий.

«Страницы в социальных сетях можно редактировать, комментарии — удалять и добавлять, умирая в компьютерной игре, ты в большинстве случаев можешь восстановить свой персонаж и продолжить. В жизни это не так, но воспитывая мозг в среде, где действия не влекут за собой последствия, мы получаем человека, просто не умеющего адекватно оценивать риски. Это связано с влиянием на область префронтальной коры головного мозга, отвечающую за логические связи — она, например, слабо развита у детей и шизофреников, которые с трудом концентрируются, легко реагируют на внешние раздражители и мыслят противоположно большинству взрослых людей — от когнитивного к чувственному.»

Приведем в пример одного рабочего, который выжил после травмы в лобной части повреждением префронтальной коры головного мозга. Человек

выздоровел, вышел на работу, но было трудно не заметить изменения его личности. Он стал давать обещания, которых не мог выполнить, заключать рискованные пари и проявлять сверхъестественное безрассудство. И не смотря на то, что он был физически вполне здоров, он не мог вести нормальную жизнь.

Еще одна опасность, таящаяся в социальных сетях – нарушение структурности мышления.

Возьмем, например, книгу. Она структурна, последовательна, есть начало, продолжение, конец. Идея и сюжет развиваются поступательно.

«Жизнь каждого из нас — хронологическая последовательность, и, разумеется, на самом деле она очень сильно отличается от того, что мы выкладываем на свою страницу в facebook. То, что беспокоит меня в информационном потоке, — возможность потери навыка мыслить последовательно, структурно. Потому что если вы знаете много вещей, но не проделываете мыслительную работу для того, чтобы их друг с другом связать, они остаются разрозненным набором фактов. Теряется навык обрабатывать информацию и создавать из нее контекст» - пишет британская исследовательница С.Гринфилд.

Легко можно научить ребенка пользоваться поиском гугла, но зачем? Ведь сначала мы должны научить его задавать и формулировать вопросы.

В шестидесятые была популярная концепция ноосферы — и может быть, мир будущего действительно будет выглядеть, как такой единый кибернетический организм, в котором идеи не принадлежат конкретному индивидууму, а практически моментально распространяются и впитываются.

Мы не можем ничего предсказать, и важно понимать, что мы должны решить сейчас, как именно мир станет развиваться. Возможно, найдется какой-то компромисс — ваша идея третьего места описывает одну из таких моделей. Люди сидят за своими компьютерами, но постоянно находятся в среде трехмерного, живого общения — это могло бы быть просто замечательно, если бы носило массовый характер. Мы сейчас в Оксфорде развиваем систему

преподавания, которая как раз построена на совместной работе, на личном контакте».

"Я боюсь многого в процессах, которые исследую, — боюсь и восхищаюсь. Это нормальная смесь чувств для исследователя — постоянное осознание того, что мир меняется на наших глазах, в наших руках. Мне часто возражают, что я уделяю слишком много внимания тому, что еще рано изучать — но ведь быстрота реакции и в науке важна, если не начать собирать этот материал сейчас, потом мы можем просто столкнуться с гораздо более серьезными проблемами."[24]

Мы так мало знаем о мозге — нам сложно точно описать, как именно он реагирует на самые базовые раздражители — но это, на мой взгляд, не причина закрывать глаза на актуальные исследования в узких областях.

Результаты исследований, проведенные Европейской комиссией «Безопасный Интернет»[25], показали, что в России 78% детей в возрасте от 9 до 16 лет имеют личный профиль в социальных сетях – этот показатель примерно на 20% больше, чем в странах Евросоюза.

Часто многие родители не видят особого вреда от того, что их ребенок имеет страничку, например Вконтакте или в Одноклассниках. Основным доводом родителей в пользу социальных сетей является то, что они создавались для объединения людей в группы единомышленников и быстрого общения. Но нельзя забывать, что социальные сети зачастую вредят психологическому здоровью и вызывают интернет-зависимость.

Социальные сети у человека отобрали живое общение. Собственно, а зачем выходить и общаться на улице, если проще написать в «аську» (ICQ) или отправить сообщение «на стену». Дополнительно теперь можно заводить неограниченное количество друзей и общаться с ними. А последствия могут

[24] Баронесса Сьюзан Гринфилд - профессор колледжа Линкольна университета в Оксфорде, фармакологического факультета, ректор университета Херриот-Ватт в Эдинбурге и член Палаты лордов. В своих научных работах она специализируется на изучении физиологии работы головного мозга и влиянии современных технологий на человеческое сознание

[25] http://ideafor.info/?p=3322

быть необратимыми – происходит переизбыток общения. У человека пропадает интерес к собеседнику. Сначала к одному, потом к другому. А потом человек теряет интерес к жизни…

Мы должны понимать, что социальные сети, особенно небезопасны для детей, поскольку содержат большое количество информации, от которой их нужно отгораживать. Думаю, не нужно объяснять, каким ребенок вырастет, если он с 8-9 лет уже смотрит порно, слушает нецензурные песни и играет на голоса (Вконтакте – голоса - это виртуальные деньги, которые вы можете потратить на приложение, подарок или поднятие рейтинга). Интеллектуальный уровень такого ребенка будет сильно отличаться от ребенка, который вместо этого читает книги и рисует. Массовая деградация школьного поколения опасна для общества.

Надо понимать, что сегодня почти все азартные игры плавно мигрировали в приложения социальных сетей. Для их оплаты используется внутренняя валюта социальной сети. Есть примеры, когда дети тратили реальные родительские деньги для поднятие своего рейтинга через смс. Задумайтесь – ведь может случиться так, что сами не заметите, как начнете отправлять смс за золотые монеты в игре. Вред для вашего кошелька очевиден.

В чем вред знакомства через социальные сети? Это же так замечательно, у ребенка появится много друзей. Конечно, вреда от этого особого нет. Разве что - нарваться на мошенника, маньяка или кибермоббера. Как мы уже говорили, надо быть внимательным, не добавлять в друзья кого попало. Конечно, общаться надо, но когда вашему ребенку начнут задавать вопросы личного характера, это тоже является сигналом для родителей. Необходимо постараться объяснить ребенку, что необходимо разделять личную жизнь и жизнь в Интернете.

Ребенку несомненно лучше погулять на улице, поиграть со сверстниками, чем попусту просиживать время в социальной сети. Большинство детей «сидят» в социальных сетях и «деградируют» час за часом. Постарайтесь объяснить

своим детям, что реальная жизнь интереснее. Несмотря на то, что социальные сети пришли в нашу жизнь и стали ее частью, они могут принести и значительный вред. Пора вернуть свою жизнь себе и детям.

Детские социальные сети – это единство медийной и маркетинговой функции, воплощенное в создании безопасной интернет-среды для детей, которая отвечает требованиям родителей и предоставляет детям инструменты для детского творчества и самовыражения в сети, общения с друзьями, мультимедийный контент, доступный через любые привычные для детей каналы коммуникации.

Детский проект «Вебики» – это интересная, познавательная, развивающая и безопасная социальная сеть-игра для детей младшего школьного возраста, специально созданная с учетом потребностей не только детей, но и их родителей.	http://www.webiki.ru	**Доступ разрешен**
Глобальная социальная сеть для детей Webkinz (имеет русскую версию), которая полностью безопасна и предлагает детям возможности социальной адаптации к взрослой жизни.	http://www.webkinz.com/ru_ru/	**Доступ ограничен**
Детский портал ВГТРК (Всероссийской государственной теле- и радио- компании) и Microsoft. Портал Бибигоша создан в рамках стратегического партнерства компаний при активном участии российского разработчика TVX Games.	http://bibigosha.ru	**Доступ ограничен**
Классная сеть для школьников. Classnet.ru – это уникальная социальная сеть для российских школьников, которая объединяет учащихся разных школ из разных городов, позволяет находить друзей по интересам	http://www.classnet.ru	**Доступ ограничен**
Твиди – детская социальная сеть от РБК (чат, игры, онлайн игры). Первая детская социальная сеть. Девиз ресурса: «Играй, Твори и Общайся!».	http://tvidi.ru	**Доступ ограничен**
Детская социальная сеть на английском. Родители имеют полный контроль над тем, что их дети делают на сайте.	http://www.imbee.com	**Доступ ограничен**
Социальная сеть Смешарики, созданная по мотивам одноименного анимационного сериала.	http://www.smeshariki.ru	**Доступ разрешен**
Совместное рисование онлайн набросков	http://my-sketch.com/	**Доступ ограничен**

Знаете ли вы, что для наших детей интернет существовал всегда?[26] То есть они не говорят, даже не мыслят категориями: «до появления интернета и после». Знаете ли вы, что до своего совершеннолетия современный ребенок отправит в среднем около 250 тысяч электронных сообщений и смс и проведет более 14 тысяч часов в интернете?

Интернет открывает безграничные возможности: для образования, развлечений и, конечно, общения с друзьями в социальных сетях. Нельзя игнорировать и опасности, ожидающие ребенка в интернете. Это могут быть спам, опасные ссылки, которые могут причинить вред компьютеру, хакеры, которые стремятся найти чужие персональные данные.

Может быть, запретить интернет, пока ваш ребенок не станет взрослым? Пожалуй, это крайняя мера, ведь для детей нет ничего желаннее, чем запретный плод. Лучше поговорить с детьми о культуре пользования интернетом и создать общие правила поведения в интернете и общения в социальных сетях.

Десять советов, как вести себя в «детских соцсетях»

1. **Начните с себя.**

Будет правильно, если ваши дети узнают о социальных сетях от вас. Создайте профиль в социальной сети вместе, расскажите о том, как о том как социальная сеть работает. Если у вашего ребенка уже есть профиль в социальной сети, попросите его показать вам свою страничку, покажите интерес к деятельности вашего ребенка в сети, добавьте его в друзья.

2. **Пароль – основа спокойствия**

Отметьте важность надежного пароля. Не стоит использовать в качестве пароля дату своего рождения, имя, простые слова или комбинации клавиш типа «123456». Попробуйте зашифровать простую понятную фразу «мы были на море в 2012», используя только первые буквы слов - получаем «мбнмв2012г». Такой пароль взломать будет очень тяжело. Чем надежнее пароль, чем меньше

[26] http://www.goodhouse.ru/family_and_children/vospitanije/deti-i-soczialnye-seti/

шансов, что аккаунт ребенка в социальной сети будет взломан. Нельзя сообщать свои пароли никому, кроме родителей. Даже близкому другу не стоит знать личный пароль, а если такое произошло, необходимо сменить пароль.

3. **Настройки приватности и конфиденциальности.**

Проследите или установите сами специальные настройки приватности для профиля вашего ребенка. Самое важное – публикуемый контент должен быть доступен только друзьям вашего ребенка.

4. **Ваша учетная запись (аккаунт) – только ваша.** Научите ребенка важному правилу - всегда выходить из учетных записей социальных сетей при выключении компьютера, особенно на общественных или школьных компьютерах. Это нужно, чтобы никто другой не смог воспользоваться аккаунтом и совершать от лица ребенка в социальной сети какие-либо действия.

5. **Твой профиль в соцсети – твое зеркало.** Объясните ребенку, что все его посты и информация, которую он публикует в социальных сетях, являются отражением его личности для других пользователей.

6. **Никакой персональной информации.** Научите ребенка никогда не публиковать личную информацию, такую, как номера телефона или домашний адрес. Просто и легко объясните, что в интернете такая информация появляться не должна, так как есть люди, которые могут воспользоваться ей в корыстных целях

7. **Только друзья.** Мы учим наших детей не вступать в разговор с незнакомыми людьми на улице. Социальная сеть – такая же многолюдная улица. Не нужно отвечать на сообщения или приглашения в друзья от незнакомых людей. Не нужно открывать сообщения от незнакомых людей, переходить по ссылкам в таких сообщениях, так как они могут содержать вирус или другой тип кибер-угрозы.

Лучше всего, если при появлении такого нежелательного сообщения, ваш ребенок обратится к вам, а вы, в этом случае, сможете либо самостоятельно

заблокировать подозрительного пользователя или обратиться в администрацию социальной сети

8. **Сначала думай, потом нажимай.** В интернете как в реальной жизни нет кнопки «вернуть назад» Статус на стене или отправленное сообщение нельзя удалить. Есть такое понятие как кэш, который хранит даже удаленную информацию, и технически грамотный человек всегда сможет найти удаленный контент. Опубликованная в интернете информация практически остается там навсегда. Поэтому важно внимательно прочитать и быть уверенным в том, что ребенок публикует или отправляет.

9. **Совет для родителей – От контроля к доверию**! Интернет, социальные сети – такая же сфера жизни как школа или общение с друзьями. Мы против того, чтобы контролировать каждый шаг ребенка в интернете, но мы уверены, что родители должны знать, что делает ребенок в интернете, соблюдает ли установленные правила – с этого и начинается доверие.

10. Используйте техническую поддержку. Для того, чтобы быть всегда на 100% уверенным в безопасности своего ребенка в интернете, существует компьютерные программы родительского контроля. Их делают практически все крупные производители антивирусных продуктов.

Например, бесплатную программу Norton Online Family можно легко скачать через интернет. Благодаря этой программе вы узнаете, в каких социальных сетях проводят время дети, что ищут в интернете, какие сайты посещают. Помимо контроля социальных сетей, программа также может следить за тем, как дети используют свои телефоны, регистрировать какие веб-сайты они посещают, установить контроль времени, которое дети проводят за компьютером. Программа присылает уведомления, когда дети пытаются сделать что-то запрещенное, например, открыть заблокированные сайты.

Заключение

Итак, мы обсудили и поняли, что - социальные сети – явление не только техническое, но скорее социально-психологическое, это удобный инструмент общения и обмена мнениями, полигон, где раскрываются невостребованные реальностью таланты. Но когда человек чрезмерно увлекается социальными сетями - это означает нехватку общения или самореализации в реальном мире, часто сетевую зависимость.

Погружение в социальные миры и сообщества совсем небезопасно, оно подобно походу в лес или погружению море, где свои законы и опасности. Особенной опасности подвергаются дети и подростки с их формирующейся личностью и психикой. И взрослые должны помочь им и поделиться своим опытом и правилами работы и жизни в социальной сети.

Для наших начинающих или далеких от техники друзей по виртуальному миру мы дали эффективные и действенные советы, проверенные временем и практикой.

Литература

1. Галкин К. Ю. Зависимость от компьютерной виртуальной реальности [Электронный ресурс] / К. Ю. Галкин. – Режим доступа к журналу: http://www .medicinform.net.

2. Жичкина А. Е. Особенности социальной перцепции в Интернете / А. Е. Жичкина // Мир психологии. – 1999. – № 3. – С. 42 – 48.

3. Мартылова О. Критерии оценки Интернет - зависимости [Электронный ресурс] / О. Мартылова. – Режим доступа к журналу: http://www.medicinform.net.

4. Мясникова И.Л . Психология отношений [Электронный ресурс] / И. Л. Мясникова . – Режим доступа у журналу : http ://www.koob.ru/myasischev-v1.

5. Раевская Е. Черты личности Интернет-зависимых и Интернет-независимых пользователей [Электронный ресурс] / Е. Раевская. – Режим доступа к журналу: http://www.flogiston.ru/search .

6. Смыслова О. Психологические последствия применения информационных технологий [Электронный ресурс] / О. Смыслова. – Режим доступа к журналу: http://www. flogiston.ru/search.

7. Харитонов А. Основные направления изменения личности современного человека в условиях информационного общества [Электронный ресурс] / А. Харитонов. – Режим доступа к журналу: http ://http://psynet.ucoz.ru

8. Чалдини Р. Психология влияния / Р. Чалдини. – СПб. : Питер, 1999. – 480 с.