Централизованные и распределенные социальные сети

А.Г. Богораз, О.Ю. Пескова

Южный федеральный университет
poy@tgn.sfedu.ru

Аннотация

Целью данной работы является анализ угроз и проблем, связанных с работой в социальных сетях. Показана типовая архитектура социальных сетей и основные проблемы, связанные с безопасностью ее использования. Выделяются прямые и косвенные угрозы. Прямые угрозы непосредственно влияют на возможность нормального и безопасного взаимодействия с социальной сетью и, в основном зависят от используемой социальной сети. Представлен относительно новый тип архитектуры, который начал использоваться в социальных сетях для решения проблем безопасности и для повышения сохранности персональных данных пользователей – частично распределенные и полностью распределенные социальные сети.

Введение

Одними из наиболее быстро развивающихся интернет-сервисов стали социальные сети. Их появление обусловлено повсеместным развитием коммуникаций, компьютеризацией общества, а также неистребимым желанием человека общаться, как со старыми друзьями, так и с новыми людьми.

Формально, социальная сеть — это веб-ориентированная платформа, используемая для создания индивидом своей сетевой идентификации — так называемого профиля, а также для создания списка «Друзей» индивида, с которыми он хочет поддерживать отношения.

Сам термин «социальная сеть» был введен в 1954 г. социологом из Манчестерской школы Джеймсом Барнсом. Во второй половине XX в. это понятие начало активно использоваться на Западе при исследованиях социальных связей и человеческих отношений, а сам термин на английском языке стал общеупотребительным.

Считается, что социальные сети начали свое распространение в 1997 году, с появлением SixDegrees.com. Это была первая социальная сеть, которая объединяла в себе такие функции, как создание своего личного профиля для самоидентификации в сети и формирование списков своих «Друзей».

В период с 1997 года по 2004 появилось большое количество социальных сетей, которые начали поддерживать различные комбинации профилей и возможность открыто указывать своих «Друзей». Такие сети как AsianAvenue, BlackPlanet и MiGente начали давать пользователям возможность создавать разные виды профилей – персональные и профессиональные профили, а также профили для знакомств.

В 2001 году была запущена социальная сеть Ryze.com для бизнеса, которая помогала бизнесменам использовать и организовывать свои бизнес-связи. Изначально создатель Ryze.com представил сеть своим друзьям — основным участникам общества бизнеса и технологий Сан-Франциско, в том числе — предпринимателям и будущим инвесторам для многих проектов социальных сетей. Стоит отметить, что участники таких проектов как Ryze.com, Tribe.net, LinkedIn и Friendster были тесно связаны между собой лично и по роду деятельности.

В 2004 году была основана крупнейшая социальная сеть в мире – Facebook. Первоначально сайт был доступен только для студентов Гарвардского университета, но начиная с сентября 2006 года доступен для всех пользователей всемирной паутины. По данным на июль 2014 года [1] аудитория Facebook составила 1.32 миллиарда пользователей, на сайте зафиксировано 125 миллиардов «дружеских связей».

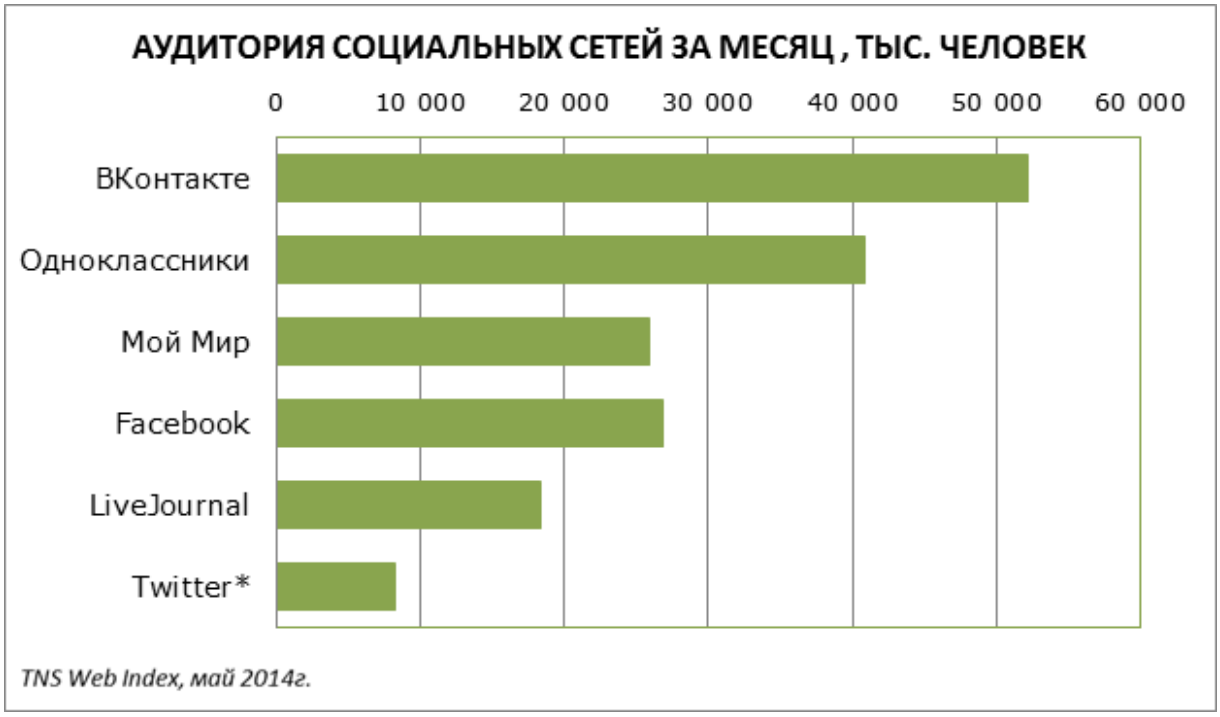
Одноклассники – первая русскоязычная социальная сеть, используемая для поиска одноклассников, выпускников, родственников, знакомых. Проект был запущен в марте 2006 года. По собственной статистике сайта, зарегистрировано более 200 миллионов пользователей, посещаемость сайта – более 44 миллионов в сутки.

Крупнейшая российская социальная сеть – Вконтакте появилась в октябре 2006 г. По данным, приведенным на сайте, зарегистрировано более 270 миллионов пользователей, более 62 миллионов посетителей заходят на сайт каждый день.

Многие социальные сети появились из сервисов, которые изначально не создавались как социальные сети, а специализировались на публикации медиа-материалов, таких как видео, фото и аудио. Примерами таких сервисов являются Flickr (публикация фото), Last.FM (сервис прослушивания музыки) и YouTube (публикация видео), которые постепенно начали добавлять к своему функционалу возможности социальных сетей.

Технологии информационного общества в науке, образовании и культуре: сборник научных статей. Материалы XVII Всероссийской объединенной конференции «Интернет и современное общество» IMS-2014, Санкт-Петербург, 19 - 20 ноября 2014 г.

В России, по данным TNS Web Index за май 2014 года [2], 80% дневной аудитории русскоязычного интернета проявляют активность в социальных сетях. Первое место по популярности социальных сетей занимает ВКонтакте, посещаемость которой в мае 2014 года выросла до 52,1 млн. человек, второе место у социальной сети «Одноклассники» с месячной аудиторией в 40,8 млн. человек (рис.1). На первом месте по количеству сообщений – также ВКонтакте, на втором месте - Twitter. (рис.2)



* Данные по Twitter экстраполированы, исходя из аудитории за день и неделю

Рис. 1. Месячная аудитория социальных сетей

* Одноклассники - данные по Топ-100 000 групп
** Facebook – оценка снизу

Рис.2. Количество русскоязычных сообщений в месяц

Во многом российский приоритет ВКонтакте по количеству сообщений связан с тем, что короткие сообщения, которые люди по всему миру предпочитают публиковать в Twitter, многие российские авторы размещают в формате статусов ВКонтакте.

Сегодня практически все распространенные социальные сети построены по централизованному принципу и имеют клиент-серверную архитектуру: сервер, отвечающий за хранение информации и организацию взаимодействия пользователей, и клиенты, позволяющие пользователю получить доступ к услугам и ресурсам социальной сети и подключающиеся для этой цели к серверу.

В целом, можно утверждать, что все социальные сети используют похожие системы защиты, основные направления из которых следующие:

- повышение защищенности серверного обеспечения и серверного оборудования;
- использование нескольких, территориально удаленных друг от друга, серверов;
- повышение уровня защищенности специального приложения или веб-сервиса для взаимодействия с социальной сетью.

Этот перечень не является исчерпывающим, но можно с уверенностью утверждать, что все перечисленные методы используются разработчиками социальных сетей для повышения уровня защищенности.

1. Основные угрозы и проблемы при работе в социальных сетях

Социальные сети представляют большой интерес с информационной точки зрения. Пользователи выкладывают в социальные сети свои персональные данные, доступ к которым открыт в любой момент времени. Эта информация представляет большую ценность не только для контактов пользователя, но для тех, кто с самыми различными целями хочет проследить за жизнью пользователя, в том числе и мошенников, и представителей правопорядка, которые работают с данными социальных сетей с прямо противоположными целями. Кроме того, социальные сети активно используются как рекламные платформы. Анализируя информацию каждого пользователя, социальная сеть определяет особенности, пристрастия, увлечения, отношения и многое другое относительно каждого отдельного пользователя этой социальной сети. В дальнейшем, эта информация может использоваться как для продажи в целях статистики, так и для определения рекламы, которую наиболее эффективно показывать пользователю.

В настоящее время актуальным являются следующие угрозы и проблемы, которые фактически относятся к любой социальной сети [3, 4]:

1. Социальные сети как источник поведенческой информации. Информация, связанная с профилем пользователя, а также информация о связях между данными и между пользователями может быть получена из социальной сети с помощью техник автоматизированного сбора или через наборы данных, предоставленные непосредственно от самих компаний. Эти материалы позволяют исследователям сетевого анализа строить модели «Дружбы», использования данных, тенденций развития и другие явные показатели, которые начались с исследования онлайн-журналов и других веб-сайтов.

2 Совмещение автономных и неавтономных социальных сетей. При этом проводимые исследования показывают, что большинство социальных сетей в основном поддерживают уже существующие социальные отношения.

3. Конфиденциальность. Конфиденциальность, в частности, имеет отношение к возможностям пользователя контролировать опубликование своих впечатлений и управлять своим социальным контекстом. В настоящее время имеются организационные и программные процедуры, которые управляют обменом межличностной информацией в социальных сетях, отправкой текста, программами мгновенной отправки сообщений, веб-сайтами объявлений, сетевыми играми, автоматизированными совместными работами и сетевым обучением. Такого рода приложения представляют собой значительную категорию социального медиа, или медиа, которое поддерживает социальное сотрудничество. Таким образом, социальные сети создают центральные хранилища личной информации. Эти архивы являются постоянными и, в то же время, постоянно пополняются. Особенностью этих архивов является не замена устаревшей информации на новую, а хранение и постоянное пополнение. Наиболее критичны проблемы конфиденциальности для молодых пользователей, которые редко задумываются о последствиях выкладывания своей информации в сети.

4. Анонимность в социальных сетях - многие пользователи социальных сетей маскируют свои реальные личности. Это может быть сделано как с помощью анонимности (полного отказа от указания имени либо выбора явного псевдонима, что встречается чаще), так и с помощью псевдоанонимности (указание ненастоящего имени). По результатам опросов пользователей социальных сетей, люди, предпочитающие анонимность и псевдоанонимность, относятся к следующим категориям:

- люди с заболеваниями, которые хотят обсудить симптомы и угрозы без их публичного упоминания;
- блогеры и активисты, участвующим в политических обсуждениях;
- учителя и работники по уходу за детьми;

- медицинские работники, в том числе специалисты в области психического здоровья;
- сотрудники правоохранительных органов;
- жертвы преследований, сексуального насилия и насилия в семье;
- дети и подростки;
- люди, ищущие работу.

Такие категории были выявлены в исследовании Бет Гивенс в статье «Информационный Бюллетень 35: Конфиденциальность в Социальных сетях: Надежность, Безопасность и Коммуникативность» [3].

Фактически, анонимность является полезным инструментом для пользователей, которые предпочитают строго разделять сетевую индивидуальность и личную жизнь. В то же время, анонимность может быть средством, которая позволит отдельным индивидам скрыть свою индивидуальность по личным причинам, а также принять участие в противоправной деятельности. Следует отметить, что определение поддельности профиля является технически сложным процессом. Однако, существует возможность выделить информацию для идентификации индивида через обновления новостей в социальных сетях, участие в группах, фотографии, сети «Друзей» или через другие косвенные идентификаторы.

5. Мошенничество в социальных сетях. Мошенники могут использовать социальные сети для связи с потенциальными жертвами. Наиболее распространенные типы мошенничеств и средств для введения в заблуждение пользователей в социальных сетях следующие:

а) Кража личных данных - использование персональной данных индивида для возможности притвориться этой личностью. Этот способ часто используется для финансовых махинаций. Информация, которую пользователи публикуют о себе в социальных сетях, может предоставить возможность получить достаточно информации для того, чтобы украсть личность. Из статьи Бет Гивенс [3] следует, что наиболее часто предметом кражи является следующая информация:

- пароли;
- информация об учетных записях в банках;
- номера кредитных карт;
- информация, которая хранится на компьютере пользователя, такая как контакты;
- получение доступа к компьютеру пользователя без его согласия;
- номер социального страхования.

б) Вредоносное программное обеспечение - это широкий спектр программ, которые устанавливаются на компьютер пользователя, часто, с помощью введения пользователя в заблуждение. Такие программы могут быстро распространяться через социальные сети с помощью установки на компьютеры пользователей без их разрешения, а также без уведомления пользователя о факте установки, что дает таким программам возможность инфицировать контакты этого пользователя. Это происходит вследствие того, что вредоносное программное обеспечение может быть получено от доверенных лиц, таких, как «Друзья», что повысит вероятность того, что пользователь воспользуется присланным адресом, и/или загрузит вредоносное обеспечение на свой компьютер.

Другие способы внедрения вредоносного ПО:

- использование укороченного адреса веб-страницы, в частности в новостях об обновлениях статуса или наборах новостей, которые на самом деле могут быть ссылкой на загружаемый файл с вредоносным программным обеспечением;
- сообщения, которые подделываются под сообщения от доверенных контактов, предлагающих пользователю воспользоваться представленным адресом, что, в свою очередь, может привести к загрузке файл или просмотру медиа-контента;
- письма, присланные по электронной почте, которые подделываются под письма от социальной сети, запрашивающие персональную информацию пользователя, или предлагающие воспользоваться предоставленной ссылкой;
- незаконные сторонние приложения — вредоносные приложения, которые могут маскироваться под сторонние приложения в социальных сетях, однако созданные специально для сбора информации о пользователях либо для инфицирования компьютера пользователя и распространения по контактам пользователя.
- ложные оповещения безопасности — приложения, которые представляются антивирусным обеспечением и информируют пользователя, что его антивирусное обеспечение устарело или была обнаружена угроза.

в) Социальная инженерия: существует значительное количество мошеннических техник, которые заставляют пользователя предоставить свою конфиденциальную информацию путем ввода его в заблуждение. Наиболее известные из них следующие:

- фишинговые атаки - это типы атак, которые используют электронные письма, мгновенные или другие виды сообщений, которые подделываются как сообщения от доверенных источников, запрашивающие различную информацию. К примеру, это может быть сообщение из банка, которое может перенаправить пользователя на поддельную страницу авторизации;
- направленная атака — это подтип фишинговых атак, при которых сообщения отправляются от доверенных лиц, таких как

коллеги, сослуживцы или «Друзья», и включают в себя адрес веб-страницы или материалы, которые рекомендуется загрузить на компьютер. Такого рода атаки возможны, в частности, благодаря другому виду техник - краже профилей пользователей социальных сетей. Адреса веб-страниц или загружаемые файлы из этих сообщений могут быть вредоносным программным обеспечением или поддельными веб-страницами, которые запрашивают конфиденциальную информацию;

- ложные приглашения — социальные сети могут использовать социальную инженерию для того, чтобы заставить пользователей чувствовать себя обязанными присоединиться к сообществу социальной сети. Такое часто происходит, когда индивид регистрируется в социальной сети, и предоставляет ей (часто непреднамеренно) доступ к списку своих контактов. Социальная сеть, получив доступ к контактам пользователя, рассылает письма, приглашающие зарегистрироваться в ней, часто указывая, что эти письма рассылаются пользователем, к контактам которого социальная сеть получила доступ;
- кража профилей — легальный профиль может быть украден теми, кто занимается их взломом, или вредоносным программным обеспечением в мошеннических целях, таких как публикование спам-сообщений, рассылка вредоносного обеспечения, кража конфиденциальных данных контактов или вымогательство денежных средств у контактов профиля. Например, от имени владельца украденного профиля могут рассылаться сообщения с просьбой о денежной помощи, уведомляющие контакты о том, что владелец счета находится за рубежом в чрезвычайной ситуации.

г) «Политика конфиденциальности»: изучение этого документа может помочь пользователю определить политику социальной сети относительно обработки информации пользователя, как личной, так и конфиденциальной. В частности, политика должна объяснить, как социальная сеть собирает и, в дальнейшем, использует информацию, о пользователях, которые посещают ее. Внимательно прочитать «Политику конфиденциальности» рекомендуется еще до прохождения процесса регистрации в социальной сети.

Отдельно следует отметить, что социальная сеть может скрыто собирать информацию о пользователях. Социальная сеть может отслеживать, где пользователь проходит авторизацию в социальную сеть, какими адресами веб-страниц он воспользовался, а также то, какими адресами веб-страниц он воспользовался после процедуры деавторизации из социальной сети. Такое скрытое отслеживание возможно благодаря служебным данным браузера, которые социальная сеть использует при взаимодействии с ним.

При изучении «Политики конфиденциальности», пользователю необходимо учитывать следующие аспекты:

- «Политика конфиденциальности» может измениться после процесса регистрации без уведомления пользователя о факте изменения;
- документ «Условия использования» может содержать такую же важную информацию, как и «Политика конфиденциальности»;
- «Политика конфиденциальности» как юридический документ, охватывает своим действием только конкретную социальную сеть. Сторонние приложения, с которыми пользователь взаимодействует при работе в социальной сети, не зависят от этого документа.

Отдельно стоит упомянуть тот факт, что «Политика конфиденциальности» обычно является объемным и сложным для понимания документом. Можно выделить набор ключевых моментов, на которые желательно обращать особое внимание при прочтении этого документа. Данный список также был выведен в работе [3]. Итак, при прочтении пользователь может руководствоваться следующим:

а) наиболее важная часть «Политики конфиденциальности» чаще всего расположена в конце документа. Таким образом, если у пользователя недостаточно времени для полноценного изучения этого документа, он может проанализировать конец документа на предмет наличия важных и ключевых моментов;

б) время хранения личной информации пользователя — следует помнить, что часть информации может быть анонимизирована после какого-то периода времени, другая часть будет через некоторое время удалена полностью, а часть может быть сохранена на неограниченный срок;

в) действия, предпринимаемые в случае удаления профиля, а также в случае смерти пользователя;

г) владелец информации, которую публикует пользователь (после публикации пользователь может потерять право на опубликованную им информацию); также необходимо изучить возможность дальнейшего использования опубликованной пользователем информации маркетологами без его явного согласия;

д) возможность написания и рассмотрения жалоб;

е) предупреждения о изменениях в Политике конфиденциальности — предупреждения публикуются по адресу веб-сайта домашней страницы или изменения публикуются исключительно по адресу веб-сайта самого документа. Стоит также изучить, каким образом пользователь уведомляется о том, что Политика конфиденциальности изменилась.

Существует угрозы, которые не имеют прямого отношения к социальной сети, но могут иметь серьезные последствия, как для компьютера пользователя, так и для профиля пользователя в социальной сети. К примерам таких угроз можно отнести:

а) уязвимости программного обеспечения, которые являются основным источником для проведения атак; уязвимости позволяют получить взломщику удаленный доступ к компьютеру пользователя, а, следовательно, к конфиденциальным личным данным;

б) невнимательность при работе в Интернете: большая часть угроз становится возможной только в том случае, если пользователь невнимательно относится к взаимодействию в социальной сети.

Таким образом, можно с уверенностью утверждать, что угрозы в социальных сетях развиваются аналогично развитию самих социальных сетей. С появлением новых технологий также появляются новые проблемы, которые могут напрямую зависеть от работы пользователя в этой социальной сети, но, в ином случае могут быть полностью независимы от возможностей пользователя.

2. Новые архитектуры — новые решения

С развитием информационных технологий начинают появляться новые типы социальных сетей. Как уже описывалось выше, большинство современных популярных социальных сетей используют клиент-серверную архитектуру. Однако существуют также социальные сети, основанные на архитектуре распределенного типа.

Распределенные социальные сети - это сети, созданные прежде всего для сохранения конфиденциальности. Личные данные пользователя хранятся исключительно на клиентской машине пользователя. Пользователь целиком и полностью определяет доступ к своим данным для любого пользователя распределенной социальной сети. В обычных социальных сетях, сервер используется для абсолютно всех клиентских действий, таких как общение, хранение информации о других пользователях и прочее. В распределенной социальной сети сервер может либо использоваться для соединения пользователей между собой, либо вообще отсутствовать. Таким образом, можно выделить 2 типа такого вида социальных сетей — клиент-серверные и полностью децентрализованные.

Клиент-серверные распределенные социальные сети работают аналогично обычным социальным сетях, но с серьезными отличиями. В распределенных социальных сетях данного типа сервер используется только для соединения клиентов между собой. Преимуществами данного решения можно назвать отсутствие необходимости хранить информацию пользователей и отсутствие доступа к личным данным пользователя. К минусам можно отнести возможность взлома сервера и последующей прослушки пользовательских коммуникаций, а также отслеживание личных данных пользователей, передаваемых между общающимися через сервер пользователями.

Полностью децентрализованные распределенные социальные сети отличаются от клиент-серверных сетей полным отсутствием сервера. Клиент такой сети устанавливается на компьютер пользователя и является как клиентом, так и сервером одновременно. Подобные сети называют еще p2p сетями. Преимуществами данного решения можно назвать:

- возможность для пользователя целиком и полностью определять доступ других пользователей к свои личным данным;
- отказоустойчивость — если один клиент будет взломан, сеть продолжит работу;
- невозможность прослушивания коммуникаций пользователей, так как соединение между клиентами шифруется;
- отсутствие возможности отследить личные данные пользователя.

Минусы:

- возможная замедленность работы по сравнению с обычными социальными сетями,
- недостаточно качественная работа на медленных каналах сети Интернет;
- необходимость пропускать через себя большое количество запросов;
- не всегда актуальная информация о состоянии частей системы.

Подобные сети только начинают полноценно развиваться благодаря появлению новых производительных и защищенных протоколов, можно привести следующие примеры проводимых разработок [5, 6]:

LifeSocial —пользователь может использовать программу для просмотра профилей из круга «друзей» в том числе и не имея доступа в Internet. Данные сохраняются на всех компьютерах сети в зашифрованном виде. Для организации поиска используется технология DHT (Distributed Hash Table), также известная по пиринговым сетям.

PeerSoN — профиль пользователя состоит из множества файлов, в каждом из которых находится некоторое поле пользовательского профиля. Пользователь задает для каждого файла права доступа, чем определяет доступность этой информации для других пользователей.

Safebook — пользовательский профиль определяется как «матрешка» - он состоит из разных уровней компьютеров, где сохранены данные пользователя, а в центре находится компьютер пользователя, который, в свою очередь, может быть на некотором уровне в «матрешке» другого пользователя. Доступ к данным пользователя может быть организован с любого

компьютера, являющегося частью «матрешки». Для организации поиска используется технология DHT (Distributed Hash Table), также известная по пиринговым сетям.

Diaspora – частично децентрализованная социальная сеть. В этой сети несколько центров. Пользователи могут выбирать сервер, которому они доверяют. Данные хранятся удаленно на сервере. Пользователи полностью доверяют информацию владельцу.

И, наконец, наиболее универсальная система Pandora, которая вышла за рамки социальных сетей – это полностью распределенная информационная система, включающая в себя функции социальной сети, средства голосового и видео общения, энциклопедии, обмена файлами, деловой системы, электронного магазина, реестра законов и стандартов, совместной работы над проектами, а также систему голосования и рейтингов. Публичные данные (например, энциклопедические статьи) свободно курсируют между узлами, приватные данные распределяются по узлам, согласно схемам доверия.

Распределенные социальные сети строятся на использовании протоколов, называемых OverIP. Под этим названием понимают протоколы передачи данных, которые упаковываются в стандартные пакеты стека TCP/IP, ничем не отличающиеся от «обычных» пакетов и используемые для передачи по открытым каналам передачи между обычными компьютерами в сети Интернет.

Иными словами, данные отправителя шифруются, упаковываются в протокол OverIP, далее получившиеся пакеты упаковываются в пакеты стека TCP/IP, а затем пересылаются по открытому каналу передачи данных. Получатель, приняв такие пакеты, распаковывает пакеты TCP/IP, затем распаковывает пакеты протокола OverIP, и уже после расшифровывает данные (рис.3).

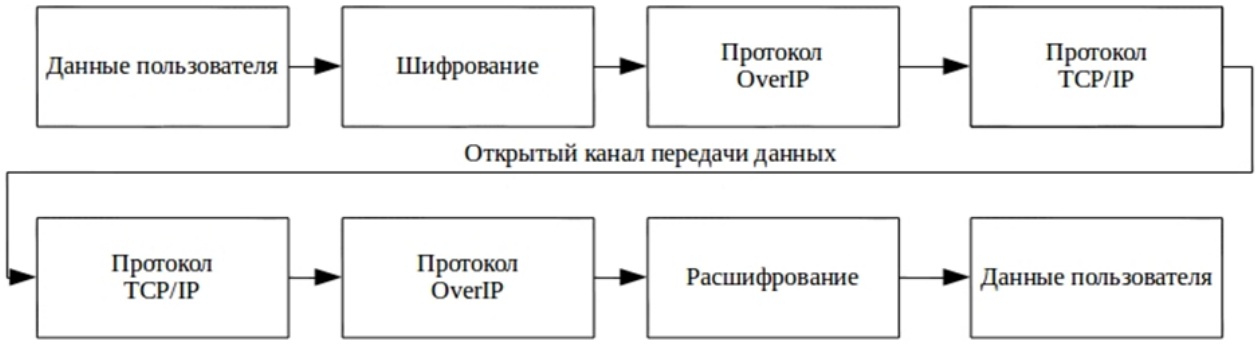


Рис.3. Передача данных с использованием OverIP

Таким образом, при передаче данных по открытому каналу достоверность получателя сообщения будет проверяться трижды. На первом этапе, когда сообщение отправляется получателю, проверяется правильность IP-адреса, указанного в заголовке пакета TCP/IP. На втором этапе, проверяется получатель сообщения в РСС, который должен знать, каким протоколом OverIP надо воспользоваться при распаковке пакетов. И на третьем этапе, получатель должен знать ключ, которым необходимо расшифровывать сообщение отправителя.

На данный момент, социальные сети, основанные на полностью децентрализованной распределенной архитектуре, считаются защищенными сами по себе, так как они построены на базе протоколов и технологий, которые изначально разрабатывались для предоставления максимальной защищенности. Но это заблуждение, поскольку угрозы и уязвимости присутствуют и здесь. Авторами начата разработка архитектуры системы защиты подобных систем.

В полностью децентрализованных социальных сетях сервер отсутствует как объект, и поэтому необходимо защищать только клиент, который одновременно является сервером для других клиентов. В случае с клиент-серверными распределенными социальными сетями, вследствие сходства архитектуры между ними и клиент-серверными социальными сетями, методы и средства защиты могут быть просто перенесены с минимальными корректировками. Аналогично необходимо защищать сервер, который можно взломать, и, в случае взлома, прослушать любые коммуникации пользователей.

Заключение

Благодаря развитию человеческого общения, социальные сети стараются гармонично развиваться и подстраиваться под нужды человеческого общения (а иногда и самостоятельно формировать эти нужды). Информационные технологии, к которым принадлежат социальные сети, сами по себе являются динамично развивающейся областью, которая своей эволюцией может отражать как современные тенденции, так и направления возможного дальнейшего развития процессов человеческого общения.

В то же время, следует отметить, что использование социальных сетей связано с определенным риском и угрозами. Социальные сети

могут использоваться не только как инструмент для общения индивидов, но и как инструмент массового сбора информации о пользователях, слежения за отдельными пользователями, формирования необходимого общественного мнения, а также мошеннических действий. Именно поэтому, необходимо понимать, что при использовании социальных сетей важно пользоваться определенными правилами и ограничениями, которые позволят предупредить нежелательные последствия, связанные с потерей личной информации.

Распределенные полностью децентрализованные социальные сети создавались для того, чтобы дать возможность пользователям управлять своей информацией, а также ее доступностью другим пользователям, что позволяет обеспечить большую защищенность всей структуры. Но и этот тип социальных сетей не может решить все проблемы, связанные с работой в сети Интернет. Авторами начата разработка архитектуры системы защиты подобных систем.

Литература

[1] Facebook Beats In Q2 With $2.91 Billion In Revenue, 62% Of Ad Revenue From Mobile, 1.32B Users [Электронный ресурс]. // TechCrunch [сайт]. URL: http://techcrunch.com/2014/07/23/facebook-q2-2014-earnings/ (дата обращения: 15.10.2014).

[2] Социальные сети в России, лето 2014: цифры, тренды, прогнозы [Электронный ресурс]. // Habrahabr [сайт]. URL: http://habrahabr.ru/company/palitrumlab/blog/230701/ (дата обращения: 15.10.2014).

[3] Givens B., Social Networking Privacy: How to be Safe, Secure and Social, PrivacyRights Clearinghouse. Empowering Consumers. Protecting Privacy [Электронный ресурс]. // Privacy Rights Clearinghouse [сайт]. URL: https://www.privacyrights.org/content/social-networking-privacy-how-be-safe-secure-and-social (дата обращения: 15.10.2014).

[4] Susan B.B., Privacy paradox: Social Networking in the United Space, First Monday, Volume 11, number 9 - USA, Illinois, Chicago. 15.08.2006 [Электронный ресурс]. // First Monday. Peer-reviewed journal on the Internet [сайт]. URL: http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394/1312 (дата обращения: 15.10.2014).

[5] Концепты P2P социальные сетей и Diaspora Privacy [Электронный ресурс]. // Habrahabr [сайт]. URL: http://habrahabr.ru/post/197434/ (дата обращения: 15.10.2014).

[6] P2P социальная сеть Pandora.- [Электронный ресурс]. // Habrahabr [сайт]. URL: http://habrahabr.ru/post/164149/ (дата обращения: 15.10.2014).

Centralized and Distributed Social Networks

A.G. Bogoraz, O.Y. Peskova

The purpose of this work is the analysis of the threats and problems connected with work on social networks. Brief historical information is given and current state of development of social networks is described. The standard architecture of social networks and the main problems connected with safety of its use is described. Direct and indirect threats are allocated. Direct threats directly influence possibility of normal and safe interaction with a social network and, generally depend on the used social network. In particular, safety issues from the point of view of storage and use of personal information of users, anonymity, and also a carelessness are touched when reading legally important documents describing politicians of work of a social network. Also rather new type of architecture which started being used on social networks for the solution of problems of safety and for increase of safety of personal information of users is described.