ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКАЯ И ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

Ненашев С.М.[1]

В наше время «онлайн» социальные сети распространены чрезвычайно широко и применяются как физическими, так и юридическими лицами. Социальные сети содержат значительный объём личной информации, вследствие чего важным аспектом их функционирования является информационная безопасность пользователей. Кроме того, возможности современных социальных сети предоставляют различным организациям (коммерческим, некоммерческим, государственным и другим) фактически прямой доступ к людям (клиентам, потенциальным сотрудникам, конкурентам и т.д.), при чём возможен отбор этих людей по набору критериев. Характер задач, решаемых юридическими лицами в социальных сетях, нередко связан с информационно–психологическим влиянием на пользователей. В статье приводится краткий обзор основных угроз информационно–технической и информационно–психологической безопасности пользователей социальных сетей. Среди угроз информационно–технической безопасности заметны как угрозы, характерные практически для любых интернет–сайтов, так и относящиеся исключительно к социальным сетям. Важность угроз информационно–психологического характера подчёркивается Доктриной информационной безопасности Российской Федерации. В статье показывается, что в реализации угроз информационно–психологической безопасности пользователей социальных сетей важную роль играют ложные личности (как управляемые вручную, так и автоматизированные «боты»). Из–за этого крайне важной в деле обеспечения информационно–психологической безопасности пользователей социальных сетей является выявление подобных ложных личностей, понимание степени достоверности указанных в пользовательском профиле данных. В завершении статьи даются рекомендации по обеспечению информационно–психологической безопасности, предлагаются меры, которые могут предприниматься в индивидуальном порядке, службами информационной безопасности предприятий, социальными сетями. Указываются разновидности программных средств, применение которых позволило бы снизить риски информационно–психологического манипулирования в социальных сетях. Такие продукты в настоящее время или малоизвестны, или недоступны на открытом рынке. Создание и развитие подобных продуктов выглядит перспективной задачей.

***Ключевые слова**: социальная сеть, информационно–техническая безопасность, информационно–психологическая безопасность, информационные угрозы, ложные личности.*

DOI:10.21681/2311-3456-2016-5-65-72

Введение

Социальная сеть (далее – СоцС), в общем случае, может быть определена как система взаимосвязей между социальными агентами (людьми или организациями). В современном русском языке под этим понятием обычно имеется в виду «онлайн» СоцС, то есть интернет-сайт, основное назначение которого – выстраивание и поддержание связей между его пользователями. В данной статье этот термин используется именно в таком значении.

СоцС позволяют зарегистрированным пользователям создавать личные страницы (так называемые «профили»), наполнять их личной информацией, публиковать текстовые и мультимедийные материалы, находить знакомых и незнакомых людей, вступать в объединения по интересам, вести переписку, а также выполнять массу иных действий.

В большинстве СоцС возможно создание пользовательских объединений, в основе которых обычно лежат интересы, участие в некотором событии, общность общественно-политических взглядов и пр. Такие объединения обычно носят название «группы».

Функциональность разных СоцС отличается, но обязательно имеются функции создания профилей и установки связей между ними. В зависимости от терминологии, принятой в конкретной СоцС, такие связи могут именоваться «дружбой», «подпиской» или иначе. В профилях пользователями публикуются их личные данные, а именно: фамилия, имя, отчество, адреса проживания, информация о предпочтениях, интересах и прочие сведения, состав и детализация которых зависит от используемой СоцС.

1 Ненашев Сергей Михайлович, аспирант кафедры «Информационная безопасность» Финансового Университета при Правительстве Российской Федерации, г. Москва, snenashev@gmail.com

Обычно пользователю предоставляется возможность ограничить доступ к личной информации в его профиле, а также к опубликованным там материалам. Модели доступа в СоцС различны [1], но на практике они во многом сводятся к тому, что пользователь обладает возможностью задать круг лиц, имеющих право читать те или иные сведения на его странице.

Социальная сеть, как объект защиты. Цель исследования

СоцС присущ ряд внутренних противоречий, влияющих на информационную безопасность пользователей, из которых наиболее важны, на наш взгляд:

– конфликт между необходимостью открывать личные данные для удобства использования функций СоцС и желанием пользователей скрыть эти данные;

– конфликт между желанием донести некоторую информацию до своих знакомых и невозможностью затем управлять доступом к этой информации;

– конфликт интересов физических и юридических лиц, являющихся пользователями СоцС.

Поиск знакомых людей, и многие другие удобные функции СоцС, тем эффективнее, чем больше пользователей предоставляют доступ к своим личным данным самой СоцС и её пользователям, фактически принося безопасность этих данных в жертву удобству – собственному и других.

Пользователям большинства СоцС доступна функция публикации чужого материала на своей странице («поделиться», «ретвит»). Опубликовав какую-то запись и предоставив доступ к ней ограниченному кругу пользователей, пользователь не может защитить её от дальнейшего нежелательного распространения.

Юридическое лицо, работая в СоцС, обычно делает это для сопровождения основных своих задач. Целями применения ими СоцС могут быть: реклама услуг и товаров [9], взаимодействие с клиентами, проверка кандидатов к приёму на работу, проверка физлиц-контрагентов, бизнес-разведка [10]. Эффективность перечисленных задач растёт вместе с ростом открытости пользовательских личных данных. Пользователю подобная открытость личных данных может нанести вред, например, потенциальный работодатель может отказаться от сотрудничества, заметив на странице кандидата сведения, порочащие его, а рекламодатель, зная личностные особенности пользователя может склонить его к нерациональным действиям, используя различные техники манипуляции.

Многие СоцС предоставляют гибкую систему управления доступом к данным, размещаемых пользователями, но в условиях открытости социального графа (или хотя бы списка друзей пользователей) подобные системы не могут гарантировать того, что лицо, не имеющее доступа к данным, не сумеет извлечь некоторые из их косвенным путём [2]. Так, если пользователь скрывает свой возраст, город проживания, места получения образования, но список его друзей открыт, такую информацию с достаточно высокой точностью можно получить анализом личных данных друзей. На рисунке (Рисунок 1) показан пример графа, ана-

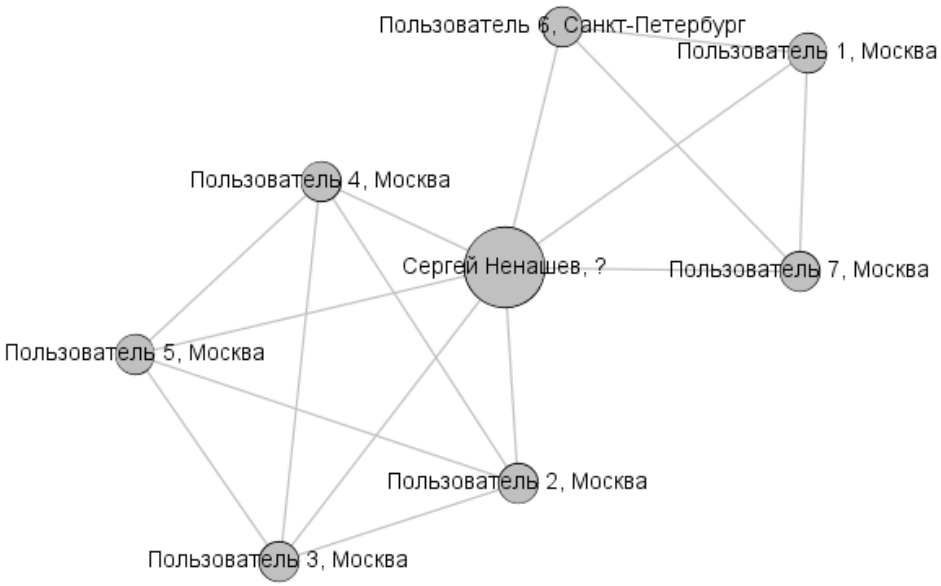

***Рис. 1**. Пример эгоцентрического социального графа, раскрывающего сведения о пользователе*

лиз которого позволяет вскрыть место проживания пользователя «Сергей Ненашев», а также выяснить, что он входит в два малосвязанных между собой коллектива.

СоцС особым образом используются физическими и юридическими лицами, целью которых является максимально широкое распространение собственного информационного влияния (общественные активисты, политические организации, благотворительные фонды и т.д.). Для таких лиц важнейшим качеством СоцС является её способность выполнять функцию особой «среды» распространения информации, где пользователи, подвергшиеся информационному воздействию, могут стать ретрансляторами этого воздействия. В отличие от традиционных средств массовой информации (печатная пресса, радио, телевидение) пользователь (зритель, слушатель) здесь становится субъектом, не только воспринимающим, но и, одновременно, передающим.

Зачастую, быстро установить настоящего автора публикации, сделанной в СоцС, невозможно. В совокупности с особенностями ретрансляции сообщений в СоцС и возможностями анонимного доступа к ней, это открыло новые возможности массового распространения лжи, пропаганды и запрещённых материалов, недоступные ранее. Противодействие такому использованию СоцС является важным аспектом информационной безопасности государства. В частности, «манипулирование информацией (дезинформация, сокрытие или искажение информации)» определено в Доктрине информационной безопасности Российской Федерации в качестве угрозы информационной безопасности, «угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России».

Обобщая, отметим, что СоцС присущи внутренние противоречия, её пользователи преследуют различные, часто противоположные, интересы в плане доступа к данным, их распространения, подтверждения их достоверности и т.д., а наличие в СоцС развитой системы управления доступом к личной информации вовсе не гарантирует действительную защищённость этих сведений. Целью данной статьи является обобщение как информационно-технических, так и информационно психологических угроз информационной безопасности, присущих СоцС, с учётом особенности их устройства и применения пользователями.

Информационно-технологические угрозы информационной безопасности пользователей СоцС

СоцС подвержены практически всем основным угрозам информационной безопасности, характерным для таких сервисов, как веб-сайты, электронная почта и системы мгновенного обмена сообщениями.

Наиболее очевидной угрозой информационной безопасности пользователей СоцС является **несанкционированный вход в СоцС**. При реализации данной угрозы злоумышленник может использовать подбор или перехват учётных данных пользователя, ложное восстановление его пароля с использованием секретного вопроса и другие способы. Многие крупные СоцС затрудняют такие атаки, применяя схемы двухфакторной аутентификации, блокирование учётной записи при попытке подбора пароля и другие схемы защиты. Последствия успешной атаки для владельца учётной записи могут быть самыми разными, а именно:

– кража личных данных владельца, включая личную переписку, фотографии и т.п.;

– использование профиля в мошеннических целях путём эксплуатации доверия друзей атакованного пользователя;

– дискредитация владельца профиля;

– деанонимизация владельца профиля.

Другие распространённые проблемы, «**кроссайтовый скриптинг**» и **распространение вирусов и «червей»,** реализуются с помощью средств информационного обмена в СоцС, а именно: публикаций на личных страницах и на страницах групп и личных сообщений. Успех «кроссайтового скриптинга» в СоцС может приводить к выполнению различных действий от лица пользователя (https://xakep.ru/2011/03/10/55008/), подменять ссылки (https://xakep.ru/2008/05/26/43751/), выполнять иные воздействия на пользователя.

Значительную угрозу пользователям СоцС представляет **фишинг**, который может реализовываться внутри СоцС (через личные сообщения и публикации в профилях) или за её пределами (электронная почта, мгновенные сообщения). При подготовке атаки могут использоваться данные из СоцС. Так поиск клиентов определённого банка может быть реализован, например, через сбор подписчиков страницы банка в СоцС. Среди найденных подписчиков могут быть выбраны наиболее уязвимые лица, имеющие в силу возрастных и образовательных особенностей низкий уровень технической грамотности. Фишинговое сообщение может содержать обращение по име-

ни и определённую личную информацию, что автоматически повысит шансы злоумышленника на успех.

Для защиты пользователей СоцС от «традиционных» угроз информационной безопасности должны использоваться обычные меры – стойкие пароли, антивирусное программное обеспечение, проверка действительности SSL-сертификатов при доступе к странице сети.

Кроме перечисленных «традиционных» угроз, пользователь СоцС сталкивается со специфической проблемой безопасности личных данных, а именно «**неявной утратой контроля над личной информацией**». Выше упоминалось **косвенное получение сведений** о пользователе путём анализа личных данных его друзей. Другим примером косвенного извлечения сведений является получение информации о перемещениях или излюбленных местах пользователя через анализ метаданных его фотографий. Некоторые СоцС предоставляют функцию поиска фотографий, сделанных в области с указанными координатами, что позволяет, например, выявлять учётные записи пользователей СоцС, проживающих или работающих по заданному адресу.

Другой путь утраты контроля за личными сведениями, а именно «**вечное» хранение данных**, характерен для многих «глобальных» информационных сервисов. У пользователя СоцС нет никакой возможности удостовериться в реальности удаления СоцС данных, удаляемых пользователем. Так, например, политика использования данных СоцС Фейсбук гласит: «Мы храним данные столько времени, сколько это необходимо, чтобы обеспечить функционирование продуктов и услуг, в том числе описанных выше, для вас и других пользователей. Информация, связанная с вашим аккаунтом, будет храниться до его удаления или же до того момента, когда нам больше не будут нужны эти данные для предоставления продуктов и сервисов.»

Активные пользователи СоцС нередко сталкиваются с **нежелательным разглашением информации третьими лицами**. Например, пользователь может быть упомянут в публикации другого пользователя, может быть отмечен на фотографии, опубликованной им. Негативные последствия подобного могут быть разнообразными – проблемы на работе или в семье из-за вскрытия утаиваемых фактов.

Информационно-психологические угрозы информационной безопасности в СоцС

Доктрина информационной безопасности России обозначает следующие виды угроз информационной безопасности:

– угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

– угрозы информационному обеспечению государственной политики Российской Федерации;

– угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

К угрозам конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возражению России относится в числе прочего:

– противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

– манипулирование информацией (дезинформация, сокрытие или искажение информации).

СоцС отлично подходят для манипулирования циркулирующей в ней информацией и для осуществления различных воздействий на сознание пользователей СоцС. Угрозы информационно-психологической безопасности пользователей СоцС (далее – УИПБ) различны и могут реализовываться с применением специальных программных средств.

Примером простейшей УИПБ может служить **социальная инженерия**. Целью такой атаки на пользователя СоцС часто является получение сведений, позволяющих выполнить некоторую традиционную атаку (например, получение ответа на «секретный вопрос»). Атака может выполняться с любой учётной записи социальной сети [8].

В основе большинства УИПБ в СоцС лежит невозможность достоверно идентифицировать пользователя СоцС. Даже если пользователь СоцС лично знаком с владельцем профиля в СоцС, о не может быть уверен в том, что профиль не взломан и не находится под контролем злоумышленника. Эта особенность используется для **социальной инженерии с использованием взломанных учёт-**

ных записей. При такой атаке злоумышленник использует доверие «друзей» пользователя взломанной учётной записи. Наиболее широко используемая схема такой манипуляции включает:

– взлом учётной записи пользователя СоцС;

– массовая рассылка друзьям сообщений с просьбой о переводе денежных средств;

– короткий диалог из общих фраз, завершающийся передачей номера анонимной банковской карты злоумышленника;

– удаление диалогов для сокрытия факта взлома учётной записи.

Взлом учётных записей наиболее популярных СоцС становится достаточно сложной задачей, поэтому злоумышленниками нередко применяется **социальная инженерия с использованием ложных личностей**. Такая атака требует заблаговременного создания злоумышленником ложной личности – копии учётной записи некоторого пользователя СоцС, и, чаще всего, добавление в «друзья» друзей копируемого пользователя. Появление дубликата обычно мотивируется тем, что доступ к прежней учётной записи утерян по той или иной причине.

Для наполнения профиля ложной личности корректными сведениями могут использоваться данные, извлекаемые из учётной записи пользователя СоцС, в которой создаётся ложная личность, или его учётных записей в других СоцС. Пользователь, присутствующий не во всех СоцС, популярных среди его друзей, более подвержен угрозе копирования его учётной записи в другую СоцС.

Целью создания ложных личностей и их инфильтрации в доверенную сеть атакуемого пользователя может быть **сбор данных ограниченного доступа с помощью ложных личностей**, а именно скрытых атрибутов профиля атакуемого пользователя, его публикаций, доступных только для «друзей» и т.д.

Ложная личность может быть полностью искусственным объектом, управляемым злоумышленником и не имеющим прототипа, и использоваться для сбора данных ограниченного доступа из закрытых групп СоцС.

Примером УИПБ, в реализации которой могут использоваться крупные коллективы ложных личностей, не имеющих явного прототипа – это **информационно-психологическое влияние на пользователей СоцС путём имитации массовости**. В качестве средства оказания влияния могут выступать: голосование, массовая публикация комментариев, выражающих одно и то же мнение, установка отметки «мне нравится» и т.д. Результатом воздействия может стать принятие пользователем СоцС решений, вредных для него, принятие точки зрения, не имеющей под собой объективного обоснования. Под влиянием эффекта массовости пользователь может изменить своё отношение к значимым вопросам его личной, экономической [3], политической жизни, чему особенно подвержена молодёжь [7].

Ложные личности могут применяться для реализации угроз **дезинформации пользователей СоцС. Для СоцС**, в отличие от традиционных средств массового распространения информации (печатная пресса, радио, телевидение) характерна децентрализованность источников информационных сообщений. Это влечёт за собой, в числе прочего, невозможность удостовериться в том, что распространяемое сообщение соответствует реальности. Использование ложных личностей, кроме, собственно, распространения ложного сообщения, позволяет имитировать интерес к публикации, наличие подтверждения данных, имеющихся в нём, и одновременно скрыть первоисточник.

Ложные личности могут применяться для усиления эффекта **поляризации и радикализации мнений пользователей СоцС**, представляющего УИПБ как для отдельных пользователей СоцС, так и, в ряде случаев, для государства в целом. Эффект связан с тем, что СоцС до немыслимого ранее уровня упростили поиск единомышленников. Носитель любой, даже самой экзотической идеи, в СоцС может найти других носителей этой идеи. Коррекция радикальных мнений и обмен аргументами между идейными оппонентами, естественные для социума, не вовлечённого в СоцС, не происходит, вместо чего повышается убеждённость носителя идеи в собственной правоте [4]. Данный эффект может быть существенно усилен правильным применением ложных личностей.

Подверженность пользователей СоцС перечисленным УИПБ вкупе с постоянным ростом аудитории СоцС привлекают к реализации данных угроз разные категории организаций, заинтересованных в информационно-психологическом воздействии на массы – крупные компании, поставляющие продукты и услуги физическим лицам, рекламные агентства, политические партии, иностранные разведки.

Выводы. Защита пользователей СоцС от УИПБ

В предыдущем разделе отмечены следующие УИПБ пользователей СоцС:

– социальная инженерия;

– социальная инженерия с использованием взломанных учётных записей;

– социальная инженерия с использованием ложных личностей;

– сбор данных ограниченного доступа с использованием ложных личностей;

– информационно-психологическое влияние на пользователей СоцС путём имитации массовости;

– дезинформация пользователей СоцС;

– усиление эффекта поляризации и радикализации мнений.

– Меры защиты пользователей СоцС от УИПБ можно разделить на три группы:

– предпринимаемые пользователями СоцС;

– предпринимаемые организациями, несущими риски ИПБ;

– предпринимаемые СоцС.

В таблице приводятся рекомендуемые меры обеспечения ИПБ пользователей:

Таблица 1.
Рекомендуемые меры обеспечения ИПБ пользователей СоцС

<table>
<tr><th></th><th>Индивидуальные меры</th><th>Меры со стороны служб ИБ</th><th>Меры со стороны СоцС</th></tr>
<tr><td>Все УИПБ</td><td></td><td rowspan="5">Информирование сотрудников об УИБ.

Проведение «учений» для сотрудников.</td><td>Информирование пользователей об УИПБ.</td></tr>
<tr><td>Социальная инженерия</td><td rowspan="3">Не следует использовать СоцС для обмена сведениями, представляющими потенциальный интерес для злоумышленников.

При необходимости обмена подобными сведениями следует использовать иные каналы связи, дающие большую степень доверия собеседнику.</td><td rowspan="5">Введение функции индикации степени доверия учётной записи, учитывающей различные показатели, такие как: способ аутентификации, стойкость пароля, факты смены сетевого положения пользователя и т.д.

Расширение функциональности подтверждения личности пользователя СоцС.</td></tr>
<tr><td>Социальная инженерия с использованием взломанных учётных записей</td></tr>
<tr><td>Социальная инженерия с использованием ложных личностей</td></tr>
<tr><td>Сбор данных ограниченного доступа с использованием ложных личностей</td><td>Закрывать доступ к любым личным данным для всех пользователей СоцС, кроме тех, в личности которых пользователь полностью уверен.
Проверять заявки на установку связи («дружбы») по другим каналам связи.</td></tr>
<tr><td>Информационно-психологическое влияние на пользователей СоцС путём имитации массовости</td><td>Заведомо не доверять кажущейся массовости любого информационного процесса, оценивая реальную массовость по данным из доверенных источников.</td><td>Отслеживание всплесков активности в группах компании в СоцС и принятие контрмер.</td></tr>
<tr><td>Дезинформация пользователей СоцС</td><td>Верификация сведений с использованием доверенных источников.</td><td>Отслеживание всплесков активности в группах компании в СоцС и принятие контрмер в форме корректирующих информационных воздействий.</td></tr>
<tr><td>Усиление эффекта поляризации и радикализации мнений</td><td>Обязательный объективный анализ противоположных мнений при формировании собственного.</td><td></td><td>Кроме предложения тем, групп, пользователей по интересам пользователя, что предлагается достаточно широко, предлагать темы, группы и пользователей.</td></tr>
</table>

Защите пользователей СоцС от УИБ поспособствовало бы появление программных средств следующих типов:

– средства индивидуальной информационно-психологической защиты;

– средства выявления автоматизированных учётных записей («ботов»);

– средства отслеживания новых связей сотрудников компании в СоцС;

– средства отслеживания активности пользователей СоцС в группах СоцС.

Заключение

Средний возраст пользователей СоцС в настоящее время по естественным причинам растёт, вместе с этим, возрастает и влиятельность пользователей СоцС в социуме. Из этого следует, что в ближайшие 20-30 лет значимость УИПБ пользователей СоцС будет возрастать, так как они будут занимать всё более высокие должности в различных организациях.

Коммерческие компании и рекламные агентства способны, в худшем случае, склонить пользователей СоцС, к принятию невыгодных для них экономических решений, но политические партии и иностранные разведки будут стремиться оказывать воздействия, целью которых будет дестабилизация экономической, социальной и политической жизни региона или целого государства [5].

Для СоцС характерны как информационно-технические, так и информационно-психологические угрозы ИБ пользователей. Для защиты от традиционных информационно-технических угроз должны использоваться традиционные средства, достаточно развитые к настоящему моменту. Специальные информационно-технические угрозы труднопреодолимы, в силу того, что являются следствиями необходимой функциональности СоцС. Различные сервисы предоставляют различные способы решения этих проблем [1].

Вопрос защиты пользователей СоцС от УИПБ сегодня проработан недостаточно, несмотря на то, что информационно-психологические воздействия на пользователей СоцС представляют в большей или меньшей степени угрозу информационной безопасности любого государства. Это подтверждается и отсутствием рынка «оборонительного» программного обеспечения индивидуального и коллективного уровней.

Научный руководитель: *Шеремет Игорь Анатольевич, доктор технических наук, профессор, i.a.sher@yandex.ru*

Литература

1. M. B. Islam, R. Iannella, J. Watson и S. Geva, «Privacy Architectures in Social Networks State-of-the-art Survey» International Journal of Information Privacy, Security and Integiry, 2015.
2. Y. Yang, J. Lutes, F. Li, B. Luo and P. Liu «Stalking Online: on User Privacy in Social Networks», 2012.
3. Глотина И.М. Информационные воздействия в социальных сетях как угроза экономической безопасности // Вестник ИЖГТУ им. М.Т. Калашникова. 2014. №3 (63). С. 99-101.
4. Y. Kim, «The contribution of social network sites to exposure to political difference: The relationships among SNSs, online political messaging, and exposure to cross-cutting perspectives» Computers in Human Bevavior, № 27, pp. 971-977.
5. Z. C. Steinert-Threlkeld, D. Mocanu, A. Vespignani and J. Fowler, «Online social networks and offline protest» EPJ Data Science, 2015.
6. Шеремет И.А. Угрозы техносфере России и противодействие им в современных условиях // Вестник академии военных наук. 2014. №1 (46).
7. Шелест В.С. Методы воздействия на общественное мнение и политическое сознание молодежи с помощью социальных сетей и сети «Интернет» // Поиск: Политика. Обществовадение. Искусство. Социология. Культура. 2012. № 5-6 (40-41). С. 138-142.
8. Фомина Н.А. Использование методов социальной инженерии при мошенничестве в социальных сетях. // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи. 2015. С. 443-453.
9. Макарова Е.А. Реклама в социальных сетях // Актуальные вопросы экономических наук. 2012. №24-1. С. 100-104.
10. Клименко С. Сбор маркетинговой информации и конкурентная разведка с использованием социальных сетей // Финансовая жизнь. 2012. № 1. С. 27-31.

INFORMATION-TECHNICAL AND INFORMATION-PSYCHOLOGICAL SECURITY OF SOCIAL-NETWORK USERS

Nenashev S.M.[2]

Online Social Networks (OSN) are widespread nowadays and used by individuals and organizations. Social networks store a large amount of personal data, so one of the most important aspects of its functioning is an information security of OSN users. Besides, direct access to the people is given to different organizations (commercial, non-commercial, public, etc.) by modern social networks capabilities. Moreover, such people (clients, potential employees, competitors) could be selected by use of criterion set. Informational-psychological impact on users is a common part of organizations' activity in online social networks due to organizations' tasks type. In this paper, we presents a short survey of the main information-technical and information-psychological threats to social network users. Threats applicable to almost every Internet-site and threats applicable to social networks only are noticeable among information-technical security threats. The Russian Federation Information Security Doctrine emphasizes the importance of the information-psychological threats. The fake identities (either manually controlled or automated «bots») plays an important role in the information-psychological threats realization, as it has been shown in the survey. Because of this, the fake identities detection and understanding of users' profile data reliability are extremely important parts of the information-psychological security ensuring task. Finally, the recommendations about users' information-psychological security ensuring are given in the article. Measures that could be taken individually by users or information security departments or social networks are given in the paper too. We describe several software types that could be useful to protect social networks users against the information-psychological manipulation. Such software is not available on the public market currently or is not widely known. The development of this software is a promising task.

***Keywords**: Social networks, information-technical security, information-psychological security, information threats, fake identities.*

References

1. M. B. Islam, R. Iannella, J. Watson и S. Geva, «Privacy Architectures in Social Networks State-of-the-art Survey» International Journal of Information Privacy, Security and Integiry, 2015.
2. Y. Yang, J. Lutes, F. Li, B. Luo and P. Liu «Stalking Online: on User Privacy in Social Networks», 2012.
3. Glotina I.M. Informacionnye vozdeystviya v socialnykh setyakh kak ugroza ekonomicheskoy bezopasnosty // Vestnik IZHGTU im. M.T. Kalashnilova. 2014. No 3 (63). P. 99-101.
4. Y. Kim, «The contribution of social network sites to exposure to political difference: The relationships among SNSs, online political messaging, and exposure to cross-cutting perspectives» Computers in Human Bevavior, № 27, pp. 971-977.
5. Z. C. Steinert-Threlkeld, D. Mocanu, A. Vespignani и J. Fowler, «Online social networks and offline protest» EPJ Data Science, 2015.
6. Sheremet I.A. Ugrozy tekhnosfere Rossii i protivodeystvie im v sovremennykh usloviyakh, Vestnik akademii voennykh nauk. 2014, No 1 (46).
7. Shelest V.S. Metody vozdeystviya na obshestvennoe mnenie I politicheskoe soznanie molodyozhi s pomoshyu socialnykh setei i seti Internet. 2012. No 5-6 (40-41). p. 138-142.
8. Fomina N.A. Ispolzovanie metodov socialnoy inzhenerii pri moshennichestve v socialnykh setyakh // Informacionnaya bezopasnost i voprosy profilaktiki kiberextremizma sredi molodyozhi. 2015. p. 443-453.
9. Makarova E.A. Reklama v socialnykh setyakh // Aktualnye voprosy ekonomicheskikh nauk. 2012. No24-1. P. 100-104.
10. Klimenko S. Sbor marketingovoy informacii i konkurentnaya razvedka s ispolzovaniem socialnykh setey // Finansovaya zhizn. 2012. No. 1 P. 27-31.

2 Sergey Nenashev, «Financial University under the Government of the Russian Federation» Information Security department post-graduate student, snenashev@gmail.com