**ISSN 2311-875X (Online)**
**ISSN 2073-2872 (Print)**

*Угрозы и безопасность*

# ОБОБЩЕННЫЙ АЛГОРИТМ РАСПРОСТРАНЕНИЯ ТАРГЕТИРОВАННОЙ ИНФОРМАЦИИ В СИСТЕМАХ СОЦИАЛЬНЫХ СЕТЕЙ

**Марина Владимировна ТУМБИНСКАЯ**

кандидат технических наук, доцент кафедры систем информационной безопасности,
Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ,
Казань, Российская Федерация
tumbinskaya@inbox.ru

**История статьи:**
Принята 28.09.2016
Принята в доработанном виде 10.11.2016
Одобрена 30.11.2016
Доступна онлайн 29.03.2017

**УДК** 004.056
**JEL:** C63

**Аннотация**

**Предмет.** Системы социальных сетей (*social network*) позволяют получить большой объем информации о пользователях – этот процесс называется «разведка на основе открытых источников». Пользователь социальных сетей самостоятельно предоставляет информацию о себе злоумышленникам, публикуя данные о своем месте работы или учебы, рассказывает о своих интересах по списку страниц и групп, в которых он состоит, и по записям, которые он публикует. Тем самым важные сведения становятся доступны для злоумышленников, организующих целевые атаки на пользователей с помощью таргетированной информации.

**Цели.** Обзор актуальных вопросов информационной безопасности в социальных системах, особенно защиты таргетированной информации, нацеленной на сохранение целостности конфиденциальных данных.

**Методология.** В работе формализован алгоритм распространения таргетированной информации в системах социальных сетей, определены его параметры, вариация которых позволит детализировать различные сценарии атак. Предложена классификация угроз информационной безопасности в социальных системах. Предложена методика защиты от таргетированной информации, распространяемой в системах социальных сетей.

**Результаты.** Детализация сценариев атак позволит выработать меры противодействия. Методика защиты от таргетированной информации, распространяемой в системах социальных сетей позволит разработать модель защиты от таргетированной информации и реализовать специальное программное обеспечение для его интегрирования в системы социальных сетей.

**Выводы.** Дана оценка эффективности применения методики защиты от таргетированной информации, распространяемой в системах социальных сетей. Предложенные решения позволят противодействовать методам информационной разведки путем использования современных методов и средств защиты информации и рекомендаций по обеспечению целостности информационных ресурсов.

**Ключевые слова:**
информационная безопасность, система социальных сетей, таргетированная информация, злоумышленник, сценарий атаки



## Введение

В настоящее время каждый человек является пользователем интернет-пространства, активно развиваются социальные информационные системы [1]. Под социальными информационными системами (*social network*) понимают информационные ресурсы, позволяющие активно взаимодействовать пользователям средствами микроблоггинга, социальных сетей, систем мгновенного обмена сообщений, электронных почтовых сервисов и др. Контент соцсетей содержит массивы информации, которой могут воспользоваться злоумышленники для различных целей, и в качестве одного из способов получения конфиденциальной информации они используют распространение таргетированной информации.

Под таргетированной информацией понимается нежелательная информация, нацеленная против определенного пользователя или группы пользователей (сообщества). Термин «таргетированная информация» близок к понятию таргетированной, то есть целевой рекламы – информации, которая предназначается определенным лицам или определенному кругу лиц так называемой целевой аудитории. Такая реклама в большинстве случаев имеет навязчивый характер и появляется в местах, где пользователь предпочел бы ее не видеть. То же самое относится и к таргетированной информации. Она представляет собой нежелательную информацию, имеет навязчивый характер и, как правило, навязывается пользователю. Очень часто распространением таргетированной информации занимаются лидеры социальных информационных систем, которые могут оказаться потенциальными злоумышленниками. Злоумышленник заинтересован в распространении таргетированной информации (то есть нежелательной информации, направленной против пользователей) через так называемых лидеров сети – пользователей

социальных информационных систем сети, которые имеют высокий уровень доверия, влияния среди большого числа пользователей данной системы или конкретного сообщества.

Информацию в социальных информационных системах можно разделить на ожидаемую и нежелательную. Ожидаемая – это та информация, которую пользователь ожидает увидеть у себя на личной странице, в своей ленте новостей и в своих личных сообщениях. Пользователь предполагает, какие сообщения станет получать, если будет добавлять в круг своего общения других пользователей и вступать в определенные сообщества. При этом по умолчанию пользователь надеется, что ему не будут присылать различные сообщения, содержащие вирусы, ссылки на сайты с вредоносным контентом, сообщения, содержащие материалы нежелательного, оскорбительного или иного негативного характера, а также ссылки на них, если только он сам не состоит в сообществах, где это приветствуется.

Согласно Доктрине информационной безопасности Российской Федерации, нежелательная информация выражается в виде:

- исполняемых документов, программ, сайтов, ссылок на информационные ресурсы, после перехода на которые, и совершая определенные действия, или без них – вызывает нарушение целостности, доступности, конфиденциальности информации на компьютере пользователя, или других ресурсов сети Интернет, или другой информации, данных, принадлежащих пользователю;
- текста, картинки (картинок), фотографий, аудио- и видеоматериалов, иных не исполняемых документов, которые могут представлять угрозу конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.

Таргетированная информация относится к нежелательной информации. В социальных информационных системах она рассматривается как угроза информационной безопасности [2].

В основе информационных систем лежит процесс обмена информацией [3]. В *табл. 1* представлена классификация угроз информационной безопасности в социальных информационных системах.

**Обобщенный алгоритм распространения таргетированной информации в социальных информационных системах**

Обобщенный алгоритм распространения таргетированной информации в социальных информационных системах можно представить в следующем виде.

1. Начало. Проникновение в социальную сеть.

2. Шаг 1. Выявление пользователя (группы пользователей), на которого будет направлена информация – объекта атаки.

3. Шаг 2. Определение влиятельного пользователя сети – лидера, потенциального распространителя таргетированной информации.

4. Шаг 3. Попытка принудить лидера распространить информацию либо распространить информацию от его лица.

5. Конец.

Под принуждением лидера к распространению таргетированной информации будем понимать попытки договориться, подкупить пользователя или же взломать аккаунт пользователя и распространять информацию от его имени (в том числе при входе на его страницу и/или через создание клона данного пользователя).

На рис. 1 и 2 представлены схемы прецедентов в нотации UML алгоритма распространения таргетированной информации в соцсетях (сценарии 1 и 2). Согласно первому сценарию, злоумышленник обращается к лидеру сети, а тот в свою очередь передает информацию пользователю системы соцсети и просит передать информацию другим пользователям. Данный пользователь передает другому пользователю системы, который, в свою очередь, передает информацию объекту атаки. Таким образом, информация доходит до объекта атаки, попутно распространяясь среди других пользователей социальной информационной системы.

По второму сценарию лидер напрямую распространяет информацию среди пользователей, которые входят в его множество входящих вершин. При этом также достигается поставленная цель – информация доходит до объекта атаки.

При этом второй способ более прост в реализации, так как распространение происходит по установленным связям (вершинам графа) и может быть оценено заранее.

Анализ социальных систем[1] [4, 5] показал, что лидерами (влиятельными пользователями) являются пользователи, которые обладают следующими параметрами:

– количество подписчиков – не менее 1 000 пользователей;

– количество постов – не менее 50;

– упоминание пользователя в постах других пользователей (частота встречаемости имени пользователя в записях остальных пользователей сети) не менее 50;

– количество оценок «мне нравится» – не менее 500;

– количество репостов сообщений пользователя – не менее 50;

– количество «друзей» пользователя – не менее 300.

Алгоритм распространения таргетированной информации в соцсетях можно представить в виде системы входящих, исходящих и внутренних параметров, которые представлены в *табл. 2*. Вариацией значений параметров *табл. 2* можно описать различные сценарии атак внутри соцсетей, в основу которых заложены алгоритмы распространения таргетированной информации.

**Методика защиты от таргетированной информации, распространяемой в системах социальных сетей**

В настоящей работе предложена формализация обобщенного сценария атаки на типичную социальную информационную систему – социальную сеть. В его основу заложен алгоритм распространения таргетированной информации, который описан с использованием методологии структурного анализа DFD [4, 6]. На *рис. 3* представлена контекстная диаграмма (уровень A0). На *рис. 4* изображены три процесса происходящие в системе соцсети, указаны хранилища данных, потоки данных, приведены внешние сущности[2] [7] – злоумышленник (источник) и объект атаки (адресат).

На *рис. 5, 6* представлены следующие уровни декомпозиции «Распространить информацию с помощью лидера» и «Выбрать стратегию распространения» соответственно.

Предложенная методика включает рекомендации по противодействию алгоритму распространения таргетированной информации в системах соцсетей, по повышению уровня защищенности персональных данных и личной информации пользователей систем.

Методика защиты от таргетированной информации, распространяемой в системах соцсетей, представлена в нотации IDEF0. На *рис. 7* представлена диаграмма A0, на которой отражены четыре функциональных блока: 1) блокировка злоумышленников; 2) защита лидеров сети; 3) усовершенствование правил фильтрации сообщений и новостей пользователя; 4) выработка рекомендаций по защите от таргетированной информации.

*Функциональный блок «Блокировка злоумышленников»* предназначен для:

– классификации пользователей на основе образов злоумышленников (то есть все пользователи классифицируются по характеристикам злоумышленников и выделяются подозрительные пользователи);

– классификации подозрительных пользователей на основе их активностей (действий) на пользователей – потенциальных злоумышленников;

– принятия решения о блокировании пользователя как определенной категории. Решение принимается по количеству действий, которые классифицируются как нежелательные, причем как по активностям в течение короткого промежутка времени, так и с учетом аккумулированной статистики пользователя.

Входящим параметром данного блока является сформированный список заблокированных пользователей.

*Функциональный блок «Защита лидеров сети»* содержит следующие функции.

1. Обучение и предостережение лидеров сети. На данном этапе необходимо вводить меры по обучению лидеров основам информационной

[1] *Майдыков А.А., Исаров О.Б.* Национальные интересы – актуальные проблемы противодействия использованию Интернета террористическими и экстремистскими организациями // Национальные интересы: приоритеты и безопасность. 2015. № 38. С. 44–51.

[2] *Мирзануров Д.Х.* Методика защиты от нежелательной информации, распространяемой в системах SOCIAL NETWORK // Символ науки. 2015. № 5. С. 48–51; *Козырь Н.С., Мальков А.А.* Корпоративная культура как элемент национальной безопасности государства // Национальные интересы: приоритеты и безопасность. 2015. № 44. С. 53–66; *Кузнецов Д.А.* Зависимость экономической и военной безопасности России от состояния защищенности стратегически важных объектов // Национальные интересы: приоритеты и безопасность. 2015. № 17. С. 52–60.

безопасности, так как в данном случае их аккаунты являются критическими ресурсами, при получении доступа к которым злоумышленник сможет распространить таргетированную информацию до значительного количества пользователей. Под информационными сообщениями понимается периодически приходящие сообщения, содержащие напоминания о необходимости соблюдать меры безопасности. Текст информационного послания может выглядеть следующим образом:

*«Уважаемый пользователь системы […]!*

*Напоминаем вам, что вы являетесь лидером данной сети, человеком, имеющим влияние на многих пользователей системы […]. Просим вас быть внимательным, и соблюдать основные правила информационной безопасности с целью предотвращения взлома вашего аккаунта.*

*Напоминаем, что любое распространение нежелательной информации является нарушением законодательства РФ и влечет за собой привлечение к ответственности.*

*С уважением, администрация системы […]».*

Кроме того, необходимо составить небольшую памятку-рекомендацию на основе используемых методов социальной инженерии и взлома.

2. Осуществление технических мер защиты. Кроме аутентификации с помощью телефона можно предложить использование антивирусов, аутентификацию с помощью аппаратных средств, предусмотреть автоматическую проверку пароля на соответствие рекомендациям информационной безопасности. Для лидеров можно установить автоматическое изменение пароля раз в месяц и вход в систему соцсети только после изменения пароля. Также к техническим мерам относятся ограничение количества рассылок от лидера сети – например, не более 1 000 пользователей в час.

3. Анализ поведения лидеров. На данном этапе представлены меры, анализирующие поведение лидеров сети. Такой анализ возможен лишь на основе реальной соцсети, где хранится вся информация о пользователе. Опираясь на информацию о времени входа/выхода, последовательности кликов – анализа карты кликов, можно построить маршруты страниц, по которым проходит пользователь. Например: страница авторизации – автоматический переброс на страницу новостей – не задерживаясь долгое время на данной странице – переход к странице с сообщениями. Дальше – ответ/письмо нескольким адресатам и переход к странице с сообществами. Далее – переход на некоторые из них, ознакомление. Далее – пост на странице или своей группе. Анализ реакции на пост. Ответные действия. Выход.

Кроме того, информация о предыдущих сессиях пользователя – время, день недели, устройство доступа, дает дополнительную информацию, и в общем случае помогает детектировать подозрительную и несвойственную активность лидера сети.

Злоумышленник же обычно ведет себя совсем по-другому:

1) отправка на сервер автоматических Get-запросов для «подгрузки» всех личных сообщений пользователя и их выгрузки;

2) отправка массовых сообщений друзьям лидера (множественные POST-запросы);

3) публикация нескольких постов с различными ссылками;

4) изменение настроек пользователей.

В таком случае возможна блокировка аккаунта и/или отправка уведомлений пользователю.

4. Выбор и комбинация соответствующих мер защиты. На данном этапе из всех предыдущих этапов выбираются те, которые подходят данному типу социальной сети.

*Функциональный блок «Усовершенствование правил фильтрации сообщений и новостей пользователя»* декомпозируется на следующие этапы.

1. Дополнительная классификация сообщений с использованием предыдущей статистики заблокированных пользователей. На данном этапе просходит анализ сообщений заблокированных пользователей, дополнение базы данных нежелательной информации, создается обучающая выборка из сообщений заблокированных пользователей.

2. Применение алгоритмов классификации для выявления таргетированной информации. На данном этапе происходит сравнение отправляемых сообщений как ожидаемой/нежелательной информации с использованием базы данных нежелательной информации и наивного баесовского классификатора. При этом учитываются оценки пользователей информации как нежелательной

(классификация). Кроме того, как уже было отмечено, учитывается уровень чувствительности к информации и происходит формирование индивидуальной модели нежелательной информации для данного конкретного пользователя. Все это создает дополнительную обучающую выборку.

3. Анализ сообщений и публичных постов лидеров. На данном этапе происходит более детальный анализ сообщений лидеров сети, причем не только исходящих, но и входящих, выявляются нежелательные сообщения. Таким образом, происходит предотвращение распространения таргетированной информации, если на предыдущих этапах система защиты не смогла распознать злонамеренные действия. В момент публикации сообщения какого-либо пользователя, содержащего ссылку, происходит автоматический переход по ней и анализ содержимого. В результате возникает незначительная задержка, в течение которой злоумышленники могут изменить первоначальное содержание ссылки.

Если ссылка признается нежелательной, переход по ней блокируется, запись удаляется. Если же ссылка признана подозрительной (ссылка на сайт с низким индексом цитирования, домены 4-го уровня и выше), то происходит периодическая проверка содержимого ссылки.

4. Создание модели фильтрации. На данном этапе создается модель фильтрации, происходит кросс-валидация модели, тестирование нескольких классификаторов (композиция классификаторов) и голосование классификаторов. Таким образом, формируются правила классификации и пополняется база данных таргетированной информации.

*Функциональный блок «Выработка рекомендаций по защите от таргетированной информации»* декомпозируется на следующие этапы.

1. Объединение результатов методики. На данном этапе все предыдущие результаты (список заблокированных пользователей, правила фильтрации, список мер защиты) объединяются для предстоящего анализа.

2. Оценка текущего состояния защиты в системе социальной сети. На данном этапе происходит оценка текущего состояния защиты по трем критериям:

– правилам блокирования пользователей;

– применяемым мерам защиты пользователей, в том числе и лидеров сети;

– применяемым правилам фильтрации и БД нежелательной информации.

На выходе данного этапа получается список текущих применяемых мер защиты в системах социальной сети.

3. Сравнение текущего уровня и новых мер защиты. На этом этапе происходит сравнительный анализ применяемых мер защиты и вновь предложенных. По приведенным критериям делается вывод, какие меры отсутствуют в текущей системе защиты.

4. Формирование необходимых мер. На данном, заключительном этапе проводится выбор наиболее экономически целесообразных мер защиты.

**Оценка эффективности применения методики защиты от таргетированной информации, распространяемой в системах социальной сети**

Для апробации предложенной методики и анализа ее эффективности выберем систему социальной сети, в которой: для блокирования пользователей не использовался подход блокирования по образам/категориям; не была предусмотрена защита лидеров сети; не применялись правила фильтрации на основе сообщений злоумышленников, анализа сообщений лидеров и отсутствовала база данных таргетированной информации. Апробация предложенной методики показала эффективность по трем критериям:

1) снижению количества пользователей в каждой категории злоумышленников путем их блокирования;

2) снижению количества получаемой таргетированной информации за счет совершенствования модели и правил фильтрации;

3) снижению количества взламываемых пользователей, в том числе и лидеров сети.

На *рис. 8, 9* представлены графики статистических данных по количеству блокируемых пользователей и распространяемой таргетированной информации от злоумышленников от времени. Среднестатистический мировой прирост пользователей в среднем составляет около 28,5 млн чел. в год[3], соответственно – 500 тыс.

[3] *Федоров П.* ВКонтакте опережает Instagram по числу зарегистрированных пользователей. URL: http://siliconrus.com/2014/01/vkontakte-operezhaet-instagram-po-chislu-zaregistrirovannyih-polzovateley

в неделю. Из них 20% являются активными пользователями (или лидерами), остальные 400 тыс. – нет; но из них 1% являются спамерами. Таким образом, по статистике обнаруживается в среднем 4 000 спамеров в неделю, а после внедрения методики системы стали блокировать 8 000 спамеров в неделю.

За неделю в среднем пользователи соцсетей рассылают примерно 7 млрд сообщений. Согласно принципу Парето «20/80», 80% сообщений генерируется 20% пользователей. Отсюда получаем, что из 228 млн пользователей – 20% (45 млн) генерирует более 5,5 млрд сообщений. При этом количество спамеров ничтожно мало – 0,000089%. Но поскольку их деятельность была неестественно активной, то можно считать, что их доля достигала 0,001% во всеобщем потоке сообщений. Соответственно, до блокирования они отправляли 5 600 млн сообщений в неделю, а после блокирования их количество уменьшилось вдвое, и они стали отправлять 2 000 000 сообщений.

На *рис. 10* представлены графики статистических данных, полученных в результате апробации предложенной методики. После внедрения методики существенно уменьшилось количество получаемой информации: с 70–80 до 35–45%.

Активность в социальных сетях подчиняется закону распределения Парето. Поскольку лидеров сети очень мало, во многих системах данный закон принимает еще более строгий вид – 2/98. Соответственно, в нашей системе лишь 2% пользователей являются лидерами сети. Таким образом, из 228 млн пользователей только 4 560 тыс. пользователей можно назвать лидерами сети.

Согласно статистике, аккаунты 60% пользователей (как обычных, так и лидеров) систем взламывались[4] [8, 9]. Так как лидеры всегда в поле зрения, то предположим, что из них в год взламывались лишь 30% – примерно 1 400 тыс. чел. Соответственно, в среднем еженедельно взламывались около 30 тыс. пользователей. После внедрения предложенной методики количество взламываемых аккаунтов сократилось в 10 раз.

Итак, раньше мы имели 20% активных пользователей – 45 млн чел. создавали 5 600 млн сообщений. Выделим среди них лидеров. Используем тот же принцип Парето – 2/98. Соответственно, 9 млн лидеров сети генерируют 4 480 млн сообщений. Так как по полученным данным лидеров в два раза меньше, получим, что 4 500 тыс. лидеров генерируют 2 240 млн сообщений в сутки. До внедрения методики количество взламываемых лидеров составляло 26 307, или 0,005846%. Но поскольку данные лидеры были взломаны, то они проявили бы активность 0,1%, что соответствует 220 400 000 сообщений за неделю, что соответствует 0,032% от общего количества сообщений. После внедрения методики количество взламываемых лидеров стало 2 500, что составляет 0,000055%. Но так как данные лидеры были взломаны, то они проявили бы активность 0,00055%, что соответствует 12 320 000 сообщений за неделю, а это 0,00176% от общего количества сообщений (*рис. 11*).

Как видно из *рис. 12*, количество распространяемой информации сильно колеблется, что вызвано значительным вкладом каждого лидера в процесс увеличения потока нежелательной информации.

**Заключение**

Предложенные в работе алгоритм распространения таргетированной информации в системах социальных сетей, а также методика защиты от таргетированной информации с использованием современных методов и средств защиты информации позволят противодействовать методам конкурентной разведки и обеспечат целостность информационных ресурсов.

[4] Eset: аккаунты соцсетей 60% пользователей рунета взламывались хакерами. URL: http://securitylab.ru/news/442581.php; *Мирзабалаева Ф.И., Алиева П.Р.* Безопасное развитие кадрового потенциала проблемного региона // Национальные интересы: приоритеты и безопасность. 2015. № 21. С. 56–66; *Яшников А.Ю., Болодурина И.П.* Выявление лидеров мнений социальной сети // Молодежный научный форум: технические и математические науки. 2016. № 5(34). С. 59–65; *Тумбинская М.В., Сафиуллина А.М.* Программное обеспечение оценивания тестовых заданий для выявления компетенций кадрового резерва с элементами защиты информации // Национальные интересы: приоритеты и безопасность. 2012. № 35. С. 42–47; *Царегородцев А.В., Макаренко Е.В.* Методика количественной оценки риска в информационной безопасности облачной инфраструктуры организации // Национальные интересы: приоритеты и безопасность. 2014. № 44. С. 30–41.

***Таблица 1***

**Классификация угроз информационной безопасности в информационных системах социальных сетей**

***Table 1***

**Classification of threats to information security in information systems of social networks**

| Тип угрозы | Характеристика угрозы |
|---|---|
| Угрозы, связанные с распространением информации – угрозы от злоумышленника | Угроза распространения вредоносной программы (личным сообщением или публично, прикрепив к записи файл) |
| | Угроза распространения ссылок на сайт, содержащих вредоносную программу, в том числе программ, следящих за пользователем, а также фишинговых сайтов – (личным сообщением или публично) |
| | Угроза распространения нежелательной информации, выраженной в виде текста, картинки (картинок), фотографий, аудио- видеоматериалов, иных не исполняемых документов, ссылок на эти документы как личным сообщением, так и публично |
| Угрозы, связанные с получением информации – угрозы для пользователя | Угроза получения вредоносной программы (в личных сообщениях, или в новостной ленте, в виде файла) |
| | Угроза получения ссылок на сайт, содержащих вредоносную программу, в том числе программ, следящих за пользователем, а также фишинговых сайтов (в личных сообщениях, или в новостной ленте) |
| | Угроза получения нежелательной информации, выраженной в виде текста, картинки (картинок), фотографий, аудио- и видеоматериалов, иных не исполняемых документов, ссылок на эти документы, как в личных сообщениях, так и в новостной ленте |
| Угрозы, связанные со взломом личной страницы пользователя | Угроза, связанная с уязвимостью в системе, позволяющая встраивать вредоносные программы в личную страницу пользователя |
| | Угроза, связанная с уязвимостью в системе, позволяющая встраивать программы слежения, в том числе позволяющие передавать данные авторизации пользователя злоумышленнику |
| | Угроза взлома личной страницы пользователя, и изменение его данных, ознакомление с личной перепиской пользователя, получение доступа к документам пользователя, разглашение этой информации, а также все перечисленные угрозы распространения нежелательной информации |

*Источник:* составлено автором

*Source:* Authoring

***Таблица 2***

**Параметры алгоритма распространения таргетированной информации в системах социальных сетей**

***Table 2***

**Parameters of the algorithm for propagating targeted information throughout social networks**

| Параметры | Описание параметра |
|---|---|
| 1. Входящие | $X = \{x_1, \ldots, x_j\}$ – массив пользователей социальной системы |
| | $x_1 = \{x_1^i \mid i = 1, n\}$ – идентификатор пользователя, где $x_1^1$ – графическое изображение пользователя; $x_1^2$ – ФИО; $x_1^3$ – логин пользователя; $x_1^4$ – возраст; $x_1^5$ – характеристика пользователя (интересы, принадлежность к сообществам, образование, место проживания и т.п.) |
| | $x_2 = \{x_2^j \mid j = 1, m\}$ – посты пользователя, где $x_2^1$ – количество постов; $x_2^2$ – количество комментариев к постам; $x_2^3$ – геолокация постов |
| | $x_3 = \{x_3^\gamma \mid \gamma = 1, s\}$ – оценки постов и сообщений, где $x_3^1$ – количество оценок других пользователей «мне нравится»; $x_3^2$ – количество репостов сообщений других пользователей сообществ; $x_3^3$ – количество сообщений в других социальных системах; $x_3^4$ – количество сообщений личного диалога пользователя |
| | $x_4 = \{x_4^\lambda \mid \lambda = 1, \beta\}$ – друзья и подписчики, где $x_4^1$ – количество подписчиков пользователя; $x_4^2$ – количество друзей пользователя |
| | $x_5 = \{x_5^\sigma \mid \sigma = 1, p\}$ – профиль страницы пользователя, где $x_5^1$ – закрытый профиль; $x_5^2$ – открытый профиль |
| | $x_6 \in 0; 1\}$ – криминальное прошлое, где $x_6 = 0$ – отсутствие признака; $x_6 = 1$ – присутствие признака |
| | $x_7 = \{x_7^k \mid k = 1, \tau\}$ – посты, где $x_7^1$ – количество постов пользователя; $x_7^2$ – ссылки на собственные сайты, другие социальные информационные системы; $x_7^3$ – количество репостов |
| | $x_8 = \{x_8^d \mid d = 1, w\}$ – цель злоумышленника, где $x_8^1$ – финансовая выгода; $x_8^2$ – самоутверждение перед самим собой; $x_8^3$ – самоутверждение перед лицом какого-либо сообщества; $x_8^4$ – возмездие знакомым пользователям, сообществу, мировой системе; $x_8^5$ – возмездие предприятию-работодателю; $x_8^6$ – преимущество в конкурентной борьбе; $x_8^7$ – удовлетворение хулиганских мотивов злоумышленника; $x_8^8$ – удовлетворение интереса, исследовательских целей злоумышленника |

| | |
|---|---|
| 2. Внутреннее состояние | $Z = \{z_1, \ldots, z_\gamma\}$ – использование методов социальной инженерии пользователем социальной системы |
| | $z_1 = \{z_1^{\,i} \mid i = 1, k\}$ – использование методов получения доступа к данным авторизации, где $z_1^{\,1}$ – использование новых уязвимостей информационных социальных систем и различных протоколов передачи данных; $z_1^{\,2}$ – использование известных уязвимостей протоколов и систем соцсети; $z_1^{\,3}$ – распространение ссылок на сайты, содержащие известные вредоносные программы; $z_1^{\,4}$ – распространение копий известных вредоносных программ; $z_1^{\,5}$ – распространение ссылок на сайты, содержащие новые, самописные вредоносные программы; $z_1^{\,6}$ – распространение копий новых, самописных вредоносных программ; $z_1^{\,7}$ – распространение ссылок на фишинговые сайты; $z_1^{\,8}$ – использование атаки прямого перебора; $z_1^{\,9}$ – использование атаки по словарю; $z_1^{\,10}$ – использование радужных таблиц; $z_1^{\,11}$ – взлом аккаунта пользователя; $z_1^{\,12}$, $z_1^{\,13}$ – взлом почтового ящика пользователя; $z_1^{\,14}$ – кража/ознакомление с файлами конфиденциальной информации путем использования доступа к сети организации; $z_1^{\,15}$ – кража/ознакомление с файлами конфиденциальной информации путем использование физического доступа к компьютеру пользователя |
| | $z_2 = \{z_2^{\,\chi} \mid \chi = 1, s\}$ – использование методов социальной инженерии для получения доступа к данным авторизации, где $z_2^{\,1}$ – использование различных предлогов для получения пароля личных знакомых; $z_2^{\,2}$ – использование легенды для получения пароля пользователя; $z_2^{\,3}$ – распространение вредоносного программного обеспечения, маскирующегося в системе защиты; $z_2^{\,4}$ – использование инфицированных физических носителей информации для получения паролей («Дорожное яблоко»); $z_2^{\,5}$ – использование подхода установления доверительных отношений; $z_2^{\,6}$ – использование шантажа; $z_2^{\,7}$ – установление договоренностей с лидером соцсети под предлогом распространения благотворительной информации социальной направленности; $z_2^{\,8}$ – установление договоренностей с лидером соцсети под предлогом распространения рекламной информации с последующим вознаграждением; $z_2^{\,9}$ – установление договоренностей с лидером соцсети для распространения информации, апеллируя к иным, скрытым мотивам – самоутверждение, обладание информацией |
| | $z_3 = \{z_3^{\,\tau} \mid \chi = 1, \omega\}$ – использование методов социальной инженерии, направленных на друзей лидера сети, где $z_3^{\,1}$ – использование методов получения доступа к данным авторизации ($z_1 = \{z_1^{\,i} \mid i = 1, k\}$) для взлома друга лидера; $z_3^{\,2}$ – установление договоренностей с другом лидера под предлогом распространения благотворительной информации социальной направленности; $z_3^{\,3}$ – установление договоренностей с другом лидера под предлогом распространения рекламной информации с обещаниями вознаграждения как лидеру, так и другу; $z_3^{\,4}$ – установление договоренностей с другом лидера для распространения информации, апеллируя к иным, скрытым мотивам (нематериальная выгода, самоутверждение, осведомленность) |
| 3. Исходящие | $Y = \{y_1, \ldots, z_p\}$ – реализованные цели злоумышленника: $y_1^{\,1}$ – материальный интерес; $y_1^{\,2}$ – самоутверждение перед самим собой; $y_1^{\,3}$ – самоутверждение перед лицом сообщества/общества; $y_1^{\,4}$ – месть знакомым; $y_1^{\,5}$ – месть сообществу; $y_1^{\,6}$ – месть мировой системе; $y_1^{\,7}$ – месть предприятию-работодателю; $y_1^{\,8}$ – преимущество в конкурентной борьбе; $y_1^{\,9}$ – хулиганство; $y_1^{\,10}$ – интерес |

*Источник:* составлено автором

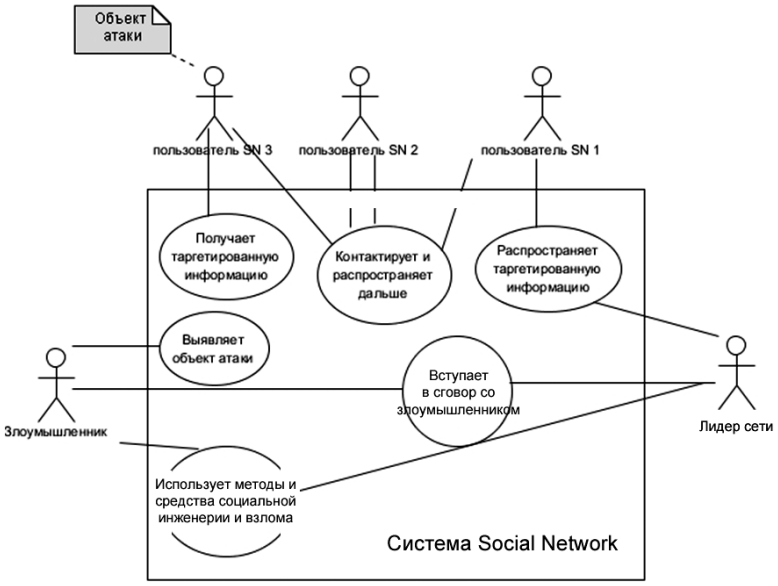
*Source:* Authoring

***Рисунок 1***

**Диаграмма прецедентов алгоритма распространения таргетированной информации (сценарий 1)**

***Figure 1***

**Diagram of cases relating to the algorithm for propagating targeted information: Scenario 1**




*Источник:* составлено автором

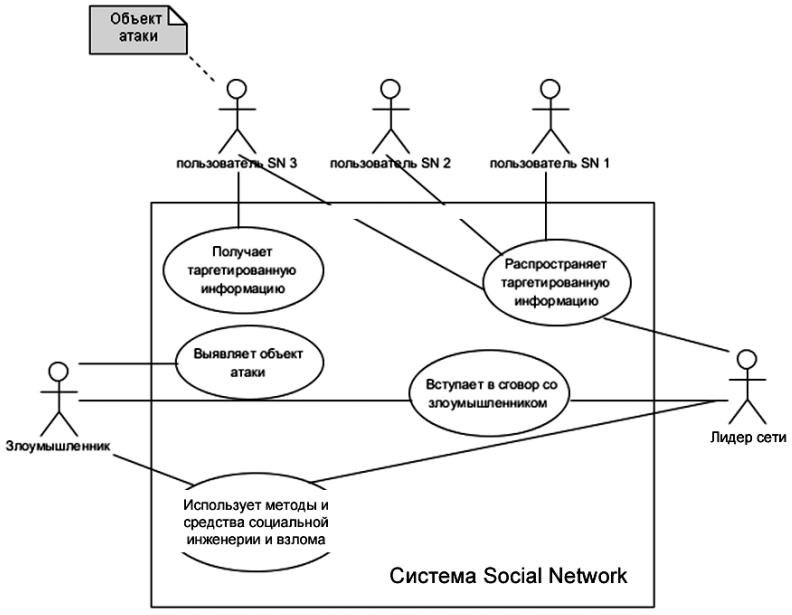
*Source:* Authoring

***Рисунок 2***

**Диаграмма прецедентов алгоритма распространения таргетированной информации (сценарий 2)**

***Figure 2***

**Diagram of cases relating to the algorithm for propagating targeted information: Scenario 2**




*Источник:* составлено автором

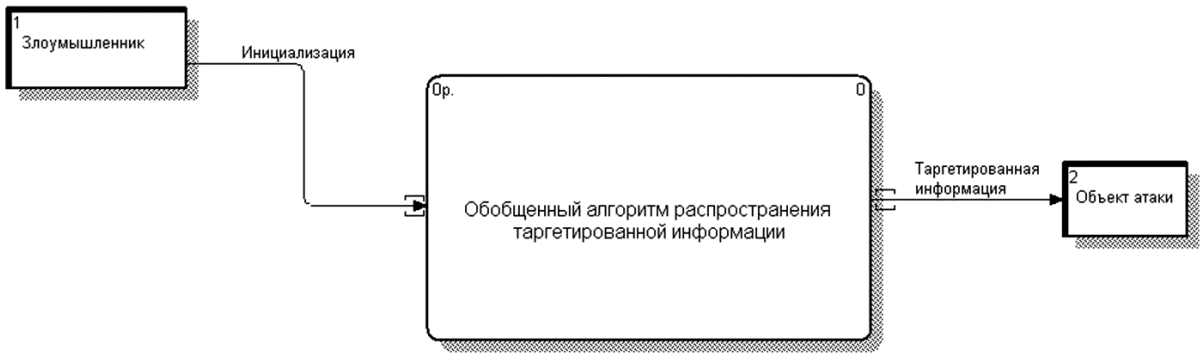
*Source:* Authoring

***Рисунок 3***

**DFD диаграмма, уровень A0 (контекстная диаграмма)**

***Figure 3***

**DFD диаграмма, уровень A-0: a contextual diagram**




*Источник:* составлено автором

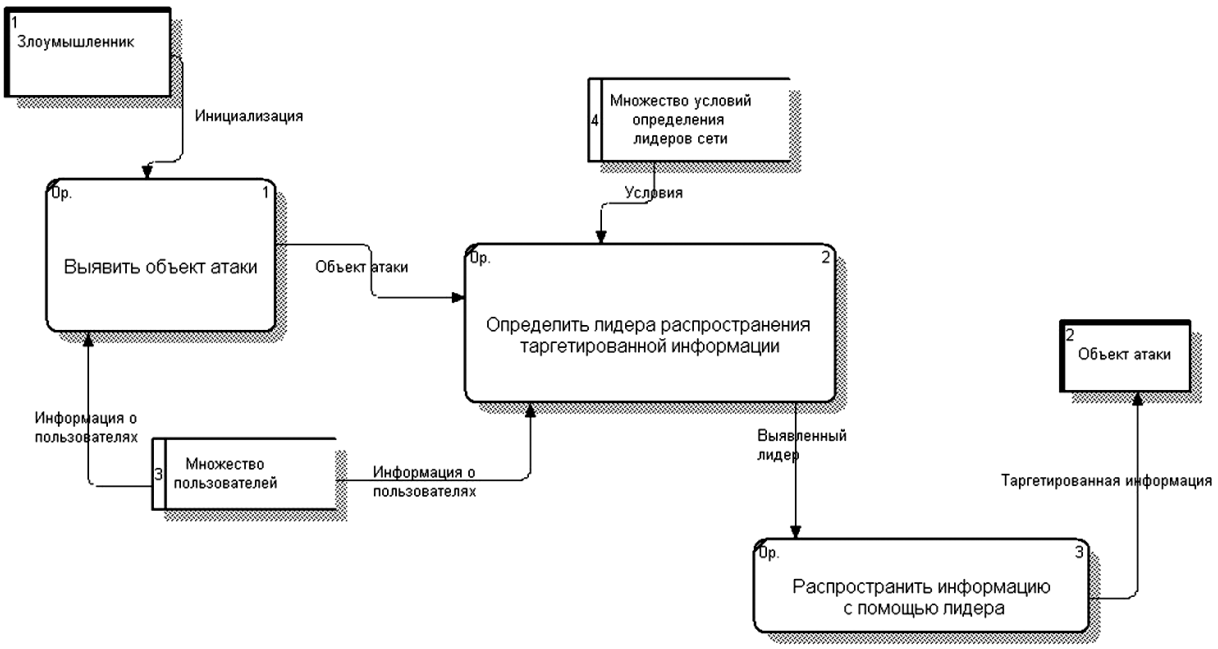
*Source:* Authoring

***Рисунок 4***

**DFD диаграмма, уровень A0**

***Figure 4***

**DFD diagram, level A0**




*Источник:* составлено автором

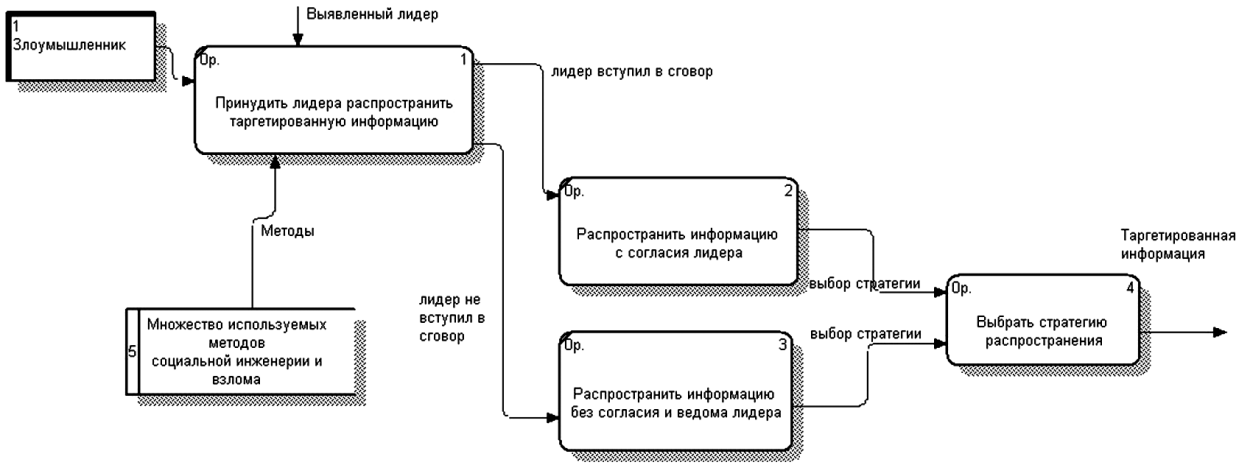
*Source:* Authoring

***Рисунок 5***

**DFD диаграмма, уровень A3**

***Figure 5***

**DFD diagram, level A3**




*Источник:* составлено автором

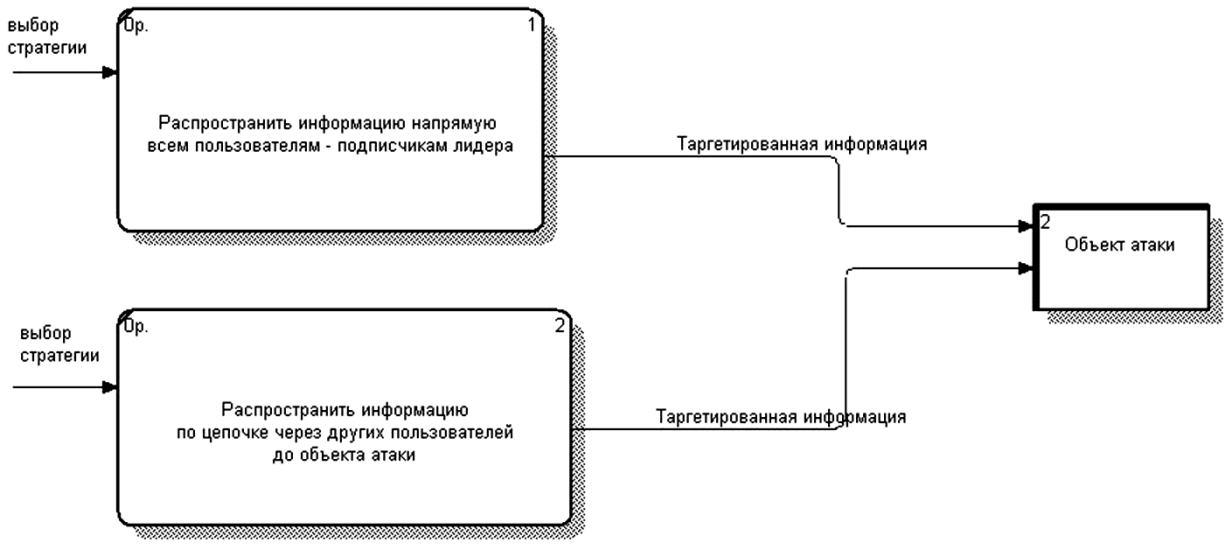
*Source:* Authoring

***Рисунок 6***

**DFD диаграмма, уровень A34**

***Figure 6***

**DFD diagram, level A34**




*Источник:* составлено автором

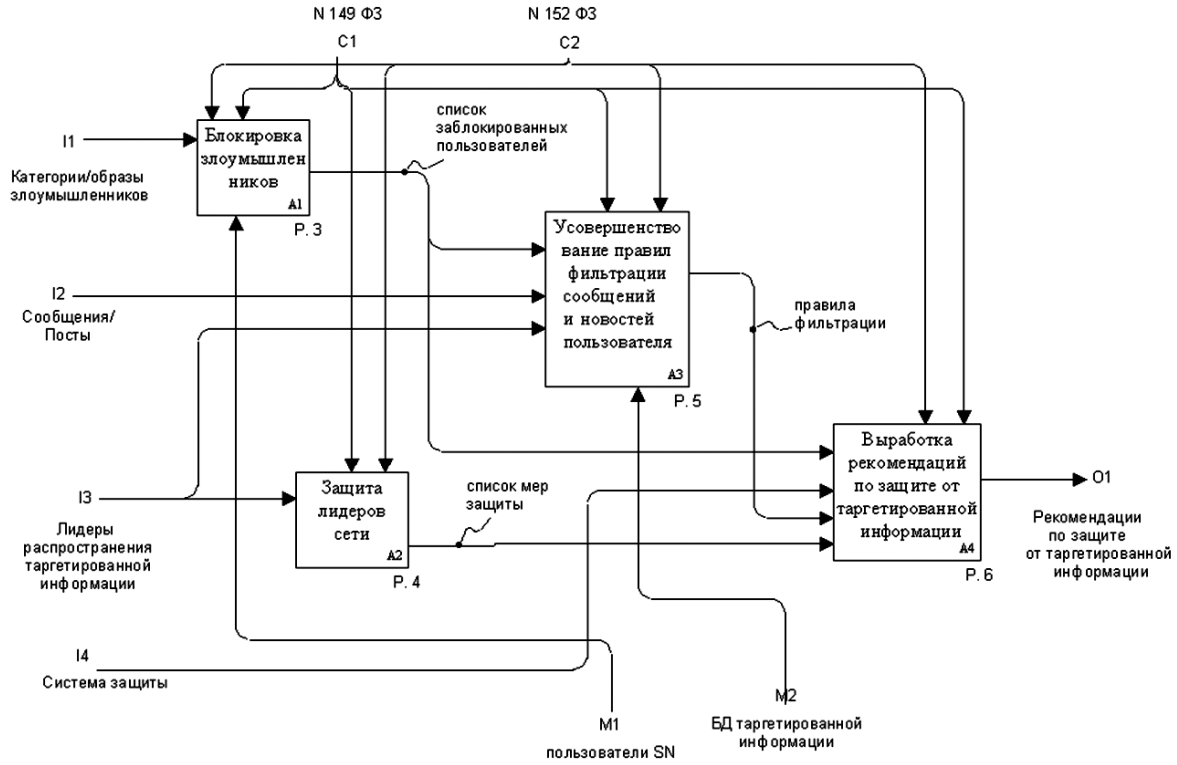
*Source:* Authoring

***Рисунок 7***

**Диаграмма IDEF0. Методика защиты от таргетированной информации (уровень A0)**

***Figure 7***

**IDEF0 diagram. The technique for protection from targeted information (level A0)**




*Источник:* составлено автором

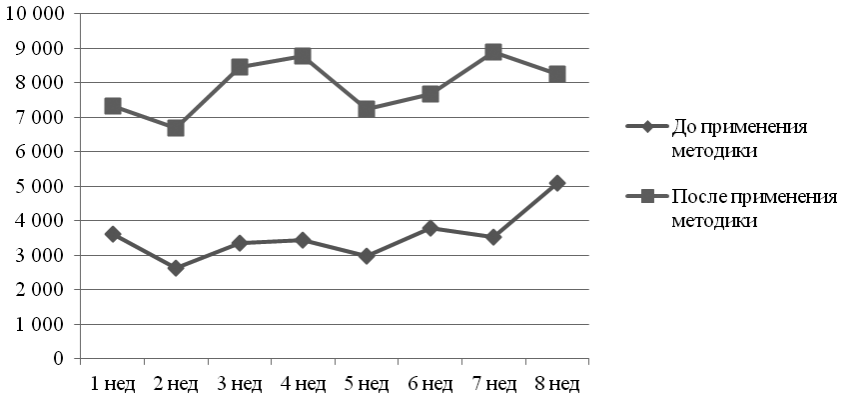
*Source:* Authoring

***Рисунок 8***

**Динамика количества блокируемых пользователей**

***Figure 8***

**Trends in the number of blocked users**




*Источник:* составлено автором

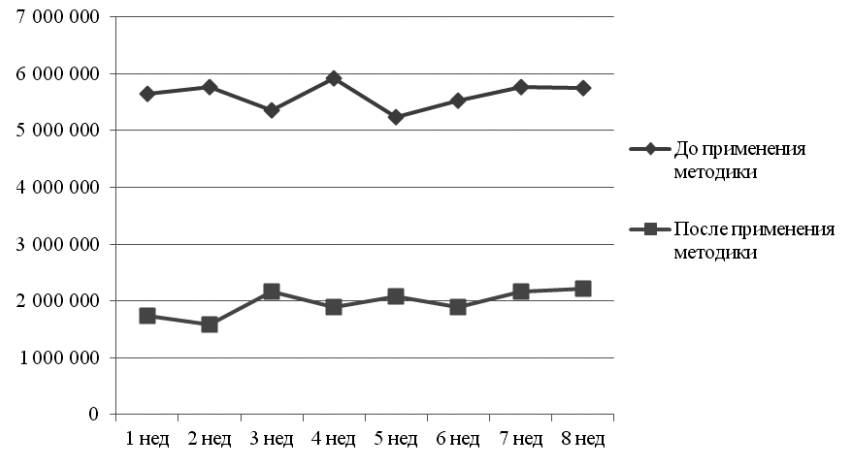
*Source:* Authoring

***Рисунок 9***

**Динамика количества распространяемой таргетированной информации от злоумышленников**

***Figure 9***

**Trends in volume of targeted information disseminated by abusers**




*Источник:* составлено автором

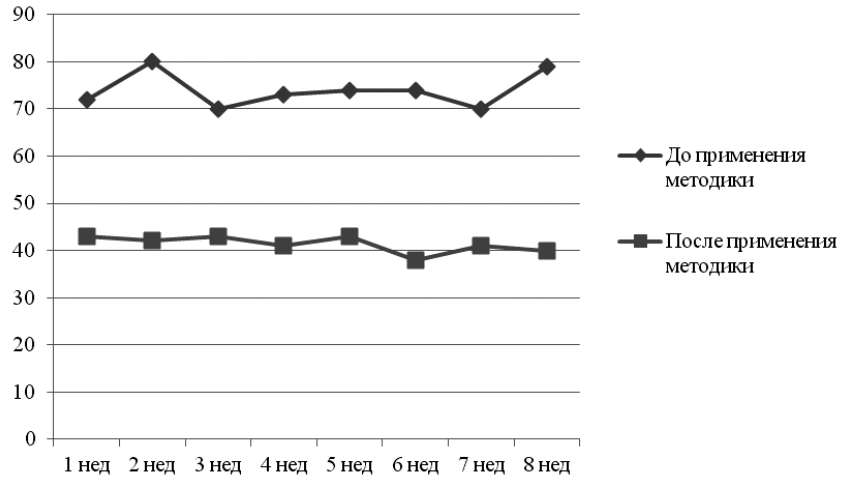
*Source:* Authoring

***Рисунок 10***

**Динамика получаемой таргетированной информации от злоумышленников**

***Figure 10***

**Trends in volume of targeted information received from abusers**




*Источник:* составлено автором

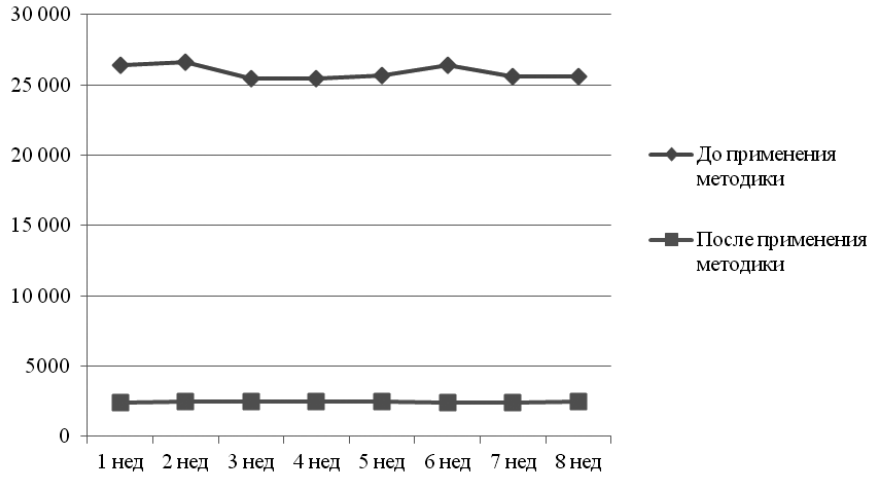
*Source:* Authoring

***Рисунок 11***

**Динамика количества взламываемых аккаунтов лидеров сети**

***Figure 11***

**Trends in the number of network leaders' accounts cracked**




*Источник:* составлено автором

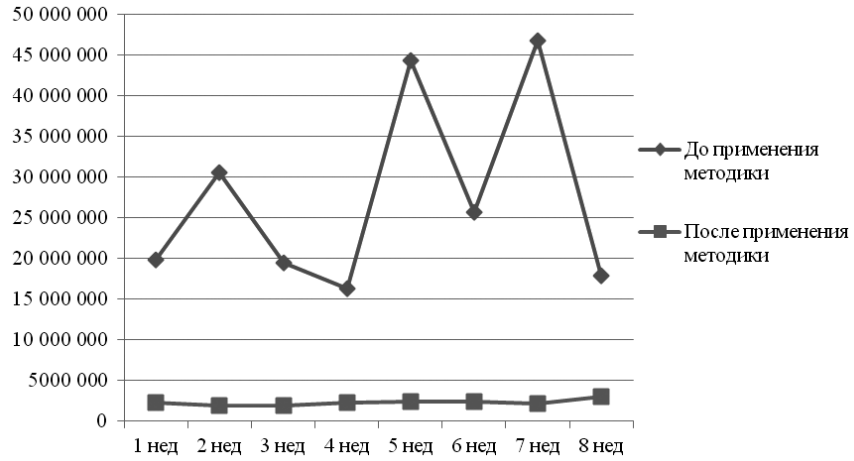
*Source:* Authoring

***Рисунок 12***

**Динамика количества распространяемой таргетированной информации от лидеров сети**

***Figure 12***

**Trends in volume of targeted information propagated by leaders of the network**




*Источник:* составлено автором

*Source:* Authoring

**Список литературы**

1. *Тультаева И.В., Каптюхин Р.В., Тультаев Т.А.* Воздействие социальных сетей на коммуникационные процессы в современном обществе // Бизнес. Образование. Право. Вестник Волгоградского института бизнеса. 2014. № 4. С. 84–88.

2. *Маркелова А.В., Козырева В.А., Сметанина О.Н.* Модели управления процессом реализации академической мобильности в вузе // Вестник Новосибирского государственного университета. Сер. Информационные технологии. 2011. Т. 9. № 2. С. 55–65.

3. *Мурзин Ф.А., Батура Т.В., Проскуряков А.В.* Программный комплекс для анализа данных из социальных сетей // Программные продукты и системы. 2015. № 4. С. 188–197.

4. *Юсупова Н.И., Ризванов Д.А., Сметанина О.Н., Еникеева К.Р.* Модели представления знаний для поддержки принятия решений при управлении сложными системами в условиях неопределенности и ресурсных ограничений: материалы IV международной конференции Information Technologies for Intelligent Decision Making Support (ITIDS'2016). Уфа: Изд-во УГАТУ, 2016. С. 24–27.

5. *Юсупова Н.И., Сметанина О.Н., Еникеева К.Р.* Иерархические ситуационные модели для СППР в сложных системах // Современные проблемы науки и образования. 2013. № 4. С. 63–68.

6. *Назаров А.Н., Галушкин А.И., Сычев А.К.* Риск-модели и критерии информационного противоборства в социальных сетях // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 7. С. 81–86.

7. *Мирзануров Д.Х.* Методика защиты от таргетированной информации, распространяемой в системах SOCIAL NETWORK // Приволжский научный вестник. 2015. № 6-1. С. 40–43.

8. *Smetanina O.N., Maximenko Z.V., Klimova A.V.* Models of education quality estimation based on fuzzy classification // Вестник Уфимского государственного авиационного технического университета. 2013. Т. 17. № 6. С. 53–56.

9. *Юсупова Н.И., Шахмаметова Г.Р.* Интеграция инновационных информационных технологий: теория и практика // Вестник Уфимского государственного авиационного технического университета. 2010. Т. 14. № 4. С. 112–118.

**Информация о конфликте интересов**

Я, автор данной статьи, со всей ответственностью заявляю о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

**ISSN 2311-875X (Online)**
**ISSN 2073-2872 (Print)**

*Threats and Security*

# A GENERIC ALGORITHM OF DISSEMINATION OF TARGETED INFORMATION IN SOCIAL NETWORKS

**Marina V. TUMBINSKAYA**

Kazan National Research Technical University n.a. A.N. Tupolev – KAI,
Kazan, Republic of Tatarstan, Russian Federation
tumbinskaya@inbox.ru

**Article history:**
Received 28 September 2016
Received in revised form
10 November 2016
Accepted 30 November 2016
Available online 29 March 2017

**JEL classification:** C63

**Keywords:** information security, social system, social networks, targeted information, abuser, attack scenario

**Abstract**

**Importance** Social networks provide massive information about users, the so called open data mining. The social network users voluntarily disclose their personal information to abusers, mentioning their work, education, interests through pages and groups, which they join, and notes they make there. Thus important data become available for abusers who organize network attacks against users through targeted information.

**Objectives** The research overviews current issues of information security in social networks, especially the protection of targeted information aimed at preserving the integrity of confidential information.

**Methods** The research relies upon the algorithm used to disseminate targeted information throughout social networks, determines its parameters, which, if varied, would help specify various scenarios of attacks. The article sets forth threats to information security in social networks and proposes protection methods.

**Results** If scenarios are specified and detailed, they will allow for counteraction measures. The method of protection from targeted information disseminated throughout social networks allows to devise anti-targeted information model and implement special-purpose software to integrate it into social systems of social networks.

**Conclusions and Relevance** The article evaluates whether the anti-targeted information methods are effectively applied. The proposed solutions will allow countering data mining through modern protection methods and tools and guidelines for integrity of information resources.



## References

1. Tul'taeva I.V., Kaptyukhin R.V., Tul'taev T.A. [An impact of social networks on communication processes in contemporary society]. *Biznes. Obrazovanie. Pravo. Vestnik Volgogradskogo instituta biznesa = Business. Education. Law. Bulletin of the Volgograd Business Institute*, 2014, no. 4, pp. 84–88. (In Russ.)

2. Markelova A.V., Kozyreva V.A., Smetanina O.N. [Models for running the academic mobility process in higher schools]. *Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya Informatsionnye tekhnologii = Novosibirsk State University Journal of Information Technologies*, 2011, no. 2, pp. 55–65. (In Russ.)

3. Murzin F.A., Batura T.V., Proskuryakov A.V. [Software package for analyzing social network data]. *Programmnye produkty i sistemy*, 2015, no. 4, pp. 188–197. (In Russ.) doi: 10.15827/0236-235X.112.188-197

4. Yusupova N.I., Rizvanov D.A., Smetanina O.N., Enikeeva K.R. [Knowledge representation models to support decision making in management of complex systems under uncertainty and restricted resources]. *Information Technologies for Intelligent Decision Making Support ITIDS'2016: materialy mezhdunarodnoi konferentsii* [Proc. Int. Sci. Conf. Information Technologies for Intelligent Decision Making Support ITIDS'2016]. Ufa, Ufa State Aviation Technical University Publ., 2016, pp. 24–27.

5. Yusupova N.I., Smetanina O.N., Enikeeva K.R. [Hierarchical situation models for DSS in complex systems]. *Sovremennye problemy nauki i obrazovaniya*, 2013, no. 4, pp. 63–68. (In Russ.) Available at: https://science-education.ru/pdf/2013/4/237.pdf.

6. Nazarov A.N., Galushkin A.I., Sychev A.K. Risk models and criteria of information confrontation in social networks. *T-Comm: Telekommunikatsii i transport = T-Comm – Telecommunications and Transportation*, 2016, no. 7, pp. 81–86. (In Russ.)

7. Mirzanurov D.Kh. [Security policy against targeted information propagated in social network systems]. *Privolzhskii nauchnyi vestnik = Volga Scientific Bulletin*, 2015, no. 6-1, pp. 40–43. (In Russ.)

8. Smetanina O.N., Maksimenko Z.V., Klimova A.V. Models of education quality estimation based on fuzzy classification. *Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta = Vestnik UGATU*, 2013, no. 6, pp. 53–56. (In Russ.)

9. Yusupova N.I., Shakhmametova G.R. [Integration of innovative information technologies: theory and practice]. *Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta = Vestnik UGATU*, 2010, no. 4, pp. 112–118. (In Russ.)

**Conflict-of-interest notification**

I, the author of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.