Для цитирования: *Тумбинская М.В. Системный подход к организации защиты от таргетированной информации в социальных сетях. Вестник Дагестанского государственного технического университета. Технические науки. 2017;44 (1):103-115. DOI:10.21822/2073-6185-2017-44-1-103-115*
For citation: *Tumbinskaya M.V. A system approach to organising protection from targeted information in social networks. Herald of Dagestan State Technical University. Technical Sciences 2017; 44 (1):103-115. DOI:10.21822/2073-6185-2017-44-1-103-115*

ТЕХНИЧЕСКИЕ НАУКИ
ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.056
DOI:10.21822/2073-6185-2017-44-1-103-115

СИСТЕМНЫЙ ПОДХОД К ОРГАНИЗАЦИИ ЗАЩИТЫ ОТ ТАРГЕТИРОВАННОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Тумбинская М.В.
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ,
420111, г. Казань, ул. К. Маркса, д.10 ООО «Подземпроект»,
e-mail: tumbinskaya@inbox.ru

***Резюме**: **Цель.** Целью исследования является формализация обобщенного алгоритма распространения таргетированной информации в социальных сетях, составляющий основу методики повышения безопасности использования личной информации. **Метод.** За основу исследования взята методика защиты от нежелательной информации, распространяемой в системах SOCIAL NETWORK. **Результат**. В статье представлена формализация алгоритма распространения таргетированной информации в социальных сетях: определены входные, выходные параметры, описаны внутренние состояния алгоритма – параметры реализации сценариев атак, вариация которых позволит их детализировать. Предложена методика защиты от таргетированной информации, распространяемой в социальных сетях, которая позволит повысить уровень защищенности персональных данных и личной информации пользователей социальных сетей, достоверность информации. **Вывод.** Результаты исследования позволят предотвратить угрозы информационной безопасности, противодействовать атакам злоумышленников, которые зачастую используют методы конкурентной разведки и социальной инженерии за счет применения мер противодействия, разработать модель защиты от таргетированной информации и реализовать специальное программное обеспечение для его интегрирования в социальные информационные системы Online Social Network. Системный подход позволит проводить внешний мониторинг событий в социальных сетях, а также осуществлять поиск уязвимостей в механизмах обмена мгновенными сообщениями для возможности реализации атак злоумышленниками. Результаты исследования позволяют на новом уровне применять активно развивающийся сегодня сетевой подход к исследованию неформальных сообществ.*

***Ключевые слова**: информационная безопасность, социальная информационная система Online Social Network, таргетированная информация, злоумышленник, сценарий атаки*

TECHICAL SCIENCE
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

A SYSTEM APPROACH TO ORGANISING PROTECTION FROM TARGETED INFORMATION IN SOCIAL NETWORKS

Marina V. Tumbinskaya
Tupolev Kazan National Research Technical University – KAI,

10 Karl Marx Str., Kazan 420111,Russia,
e-mail: tumbinskaya@inbox.ru

Abstract. Objectives *The aim of the study is to formalise a generalised algorithm for the distribution of targeted information in social networks, serving as the basis for a methodology for increasing personal information security.* ***Method*** *The research is based on the methodology of protection from unwanted information distributed across social network systems.* ***Results*** *The article presents the formalisation of an algorithm for the distribution of targeted information across social networks: input and output parameters are defined and the algorithm's internal conditions are described, consisting of parameters for implementing attack scenarios, which variation would allow them to be detailed. A technique for protection from targeted information distributed across social networks is proposed, allowing the level of protection of personal data and information of social networks users to be enhanced, as well as the reliability of information increased.* ***Conclusion*** *The results of the research will help to prevent threats to information security, counteract attacks by intruders who often use methods of competitive intelligence and social engineering through the use of countermeasures. A model for protection against targeted information and implement special software for its integration into online social network social information systems is developed. The system approach will allow external monitoring of events in social networks to be carried out and vulnerabilities identified in the mechanisms of instant messaging, which provide opportunities for attacks by intruders. The results of the research make it possible to apply a network approach to the study of informal communities, which are actively developing today, at a new level.*

Keywords: *information security, online social networks, social information systems, targeted information, intruders, attack scenario*

Введение. В настоящее время каждый человек является пользователем интернет-пространства, активно развиваются социальные информационные системы Online Social Network – социальные сети. Социальные сети характеризуются простотой реализации продвижения бизнеса, распространения рекламы товаров и услуг, досуга, хобби, личного общения и обмена информацией, тем самым являясь открытым источником информации для злоумышленников. Злоумышленники в качестве одного из способов получения конфиденциальной информации используют распространение таргетированной информации [1] в социальных сетях.

Под таргетированной информацией понимается нежелательная информация, содержащаяся в информационных сообщениях пользователя или группы пользователей (сообщества) социальной сети [1]. Для своих целей злоумышленники могут использовать лидеров социальной сети. Чаще всего лидеры имеют высокий уровень доверия среди большого числа пользователей социальной сети или сообщества, либо являются создателями (администраторами) сети или сообщества [2 – 5].

В работах [6, 7] рассмотрены алгоритм распространения нежелательной информации в системах Social Network, который представлен в виде реализации одной из возможных диаграмм прецедентов с использованием языка UML, что недостаточно для понимания его работы, методика защиты от таргетированной информации, которая представлена тремя этапами вербального описания и не отражает процесса взаимодействия с алгоритмом.

Постановка задачи. В отличие от работ [6, 7], в статье автором сделана попытка формализации обобщенного алгоритма распространения таргетированной информации в социальных сетях путем определения входных, выходных и внутренних состояний алгоритма, которые заложены в основу методики защиты от таргетированной информации.

Методы исследования. Достоинством предложенной автором статьи методики в отличие от методики, представленной в работах [6, 7] является ее дополнение, модификация функциональных блоков и их детализация. Кроме того, автором предложена структурная схема методики защиты от распространения таргетированной информации в социальных сетях,

которая отражает параметрические взаимосвязи. Достоинством методики является практическая значимость, а в статье представлены результаты ее успешной апробации. Отличительной особенностью от работы автора Д.Х. Мирзанурова [7] является предложенный анализ методов выявления влиятельных пользователей сети в системах Social Network, на основе зарубежных публикаций ученых.

Научная новизна работы заключается в формализации обобщенного алгоритма распространения таргетированной информации в социальных сетях, заложенный в основу методики защиты от таргетированной информации, которая позволит повысить безопасность использования личной информации в социальных сетях.

Обсуждение результатов. Обобщенный алгоритм распространения таргетированной информации в социальных сетях

В работе предложен обобщенный алгоритм распространения таргетированной информации в социальных сетях, который можно представить в виде:

1. Начало.
2. Шаг 1: Выявить пользователя (группу пользователей), для которого предназначена таргетированная информация - объект атаки.
3. Шаг 2: Определить влиятельного пользователя – лидера распространения таргетированной информации.
4. Шаг 3. Принудить лидера распространить таргетированную информацию или распространить информацию от лица лидера, используя методы социальной инженерии.
5. Конец.

Алгоритм распространения таргетированной информации в системах Online Social Network можно представить в виде системы входных, выходных и внутренних параметров, вариация которых позволит формализовать различные сценарии атак на социальные сети [8 – 9].

Формализация обобщенного алгоритма распространения таргетированной информации в социальных сетях

Входные параметры: $X = \{x_1,...,x_j\}$ – пользователи социальной системы Social Network, $x_1 = \{x_1^i \mid i = \overline{1,n}\}$ – 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 социальных сетей, образование, место проживания и т.п.); $x_2 = \{x_2^j \mid j = \overline{1,m}\}$ – посты пользователя социальной сети, где x_2^1 – количество постов, x_2^2 – количество комментариев к постам, x_2^3 – геолокация постов; $x_3 = \{x_3^\gamma \mid \gamma = \overline{1,s}\}$ – 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 сетях, x_3^4 – количество сообщений личного диалога пользователя; $x_4 = \{x_4^\lambda \mid \lambda = \overline{1,\beta}\}$ – друзья и подписчики, где x_4^1 – количество подписчиков пользователя, x_4^1 – количество друзей пользователя; $x_5 = \{x_5^\sigma \mid \sigma = \overline{1,p}\}$ – профиль страницы пользователя, где x_5^1 – закрытый профиль, x_5^2 – открытый профиль; $x_6 \in \{0;1\}$ – криминальное прошлое, $x_6 = 0$ - отсутствие признака, $x_6 = 1$ – присутствие признака; $x_7 = \{x_7^k \mid k = \overline{1,\tau}\}$ – посты, где x_7^1 – количество постов пользователя, x_7^2 – ссылки на собственные сайты, другие социальные сети, x_7^3 – количество репостов; $x_8 = \{x_8^d \mid d = \overline{1,w}\}$ – цель злоумышленника, где x_8^1 – финансовая выгода, x_8^2 – самоутверждение перед самим собой, x_8^3 – самоутверждение перед лицом какого-либо сообщества/общества социальные сети, 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, x_8^8 – удовлетворение интереса, исследовательских целей.

Параметры внутренних состояний алгоритма: $Z = \{z_1,...,z_\gamma\}$ – использование методов социальной инженерии пользователем социальной сети: $z_1 = \{z_1^i \mid i = \overline{1,k}\}$ – использование методов получения доступа к данным авторизации, где z_1^1 – использование новых уязвимостей социальной сети и различных протоколов передачи данных, z_1^2 – использование известных уязвимостей и протоколов передачи данных, 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} – – взлом почтового ящика пользователя, z_1^{13} – кража/ознакомление с файлами конфиденциальной информации путем использования доступа к сети организации, z_1^{14} – кража/ознакомление с файлами конфиденциальной информации путем использование физического доступа к компьютеру пользователя; $z_2 = \{z_2^\chi \mid \chi = \overline{1,s}\}$ – 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 социальной сети под предлогом распространения благотворительной информации социальной направленности, z_2^8 – установление договоренностей с лидером социальной сети под предлогом распространения рекламной информации с последующим вознаграждением, z_2^9 – установление договоренностей с лидером системы Social Network для распространения информации, апеллируя к иным скрытым мотивам - самоутверждение, обладание информацией; $z_3 = \{z_3^\tau \mid \tau = \overline{1,\omega}\}$ – использование методов социальной инженерии, направленных на друзей лидера социальной сети, где z_3^1 – использование методов получения доступа к данным авторизации ($z_1 = \{z_1^i \mid i = \overline{1,k}\}$) для взлома друга лидера, z_3^2 установление договоренностей с другом лидера Social Network под предлогом распространения благотворительной информации социальной направленности, z_3^3 – установление договоренностей с другом лидера социальной сети под предлогом распространения рекламной информации с обещаниями вознаграждения, как лидеру, так и другу, z_3^4 – установление договоренностей с другом лидера социальной сети для распространения информации, апеллируя к иным скрытым мотивам (нематериальная выгода, самоутверждение, осведомленность) [10 – 12].

Выходные параметры: $Y = \{y_1,...,y_p\}$ – 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.

В работе детализация внутренних состояний обобщенного алгоритма распространения таргетированной информации в социальных сетях заложена в основу методики защиты от таргетированной информации.

Рассмотрим алгоритм распространения таргетированной информации в социальных сетях с использованием лидера сообщества (основные параметры: z_2^7, z_2^8, $z_3 = \{z_3^\tau \mid \tau = \overline{1,\omega}\}$). Формализация обобщенного алгоритма представлена с использованием методологии структурного анализа DFD, который включает 3 основные шага (рис. 1), а также хранилища данных, потоки данных, указаны внешние сущности – злоумышленник (источник) и объект атаки (адресат).

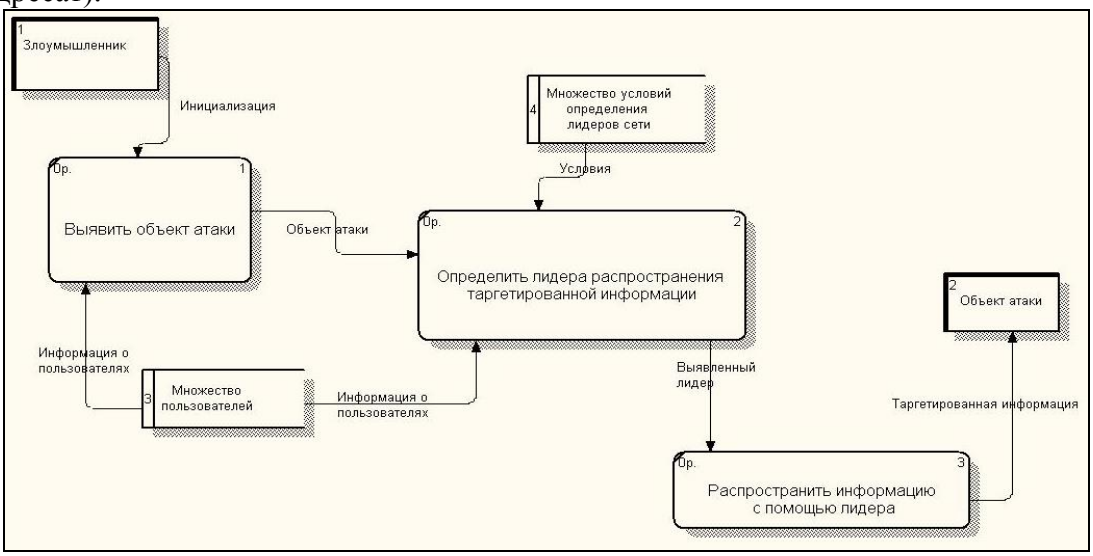

Рис.1.DFD диаграмма формализации обобщенного алгоритма распространения таргетированной информации в социальных сетях
Fig.1.DFD diagram of formalization of the generalized algorithm of distribution of the targeted information in social networks

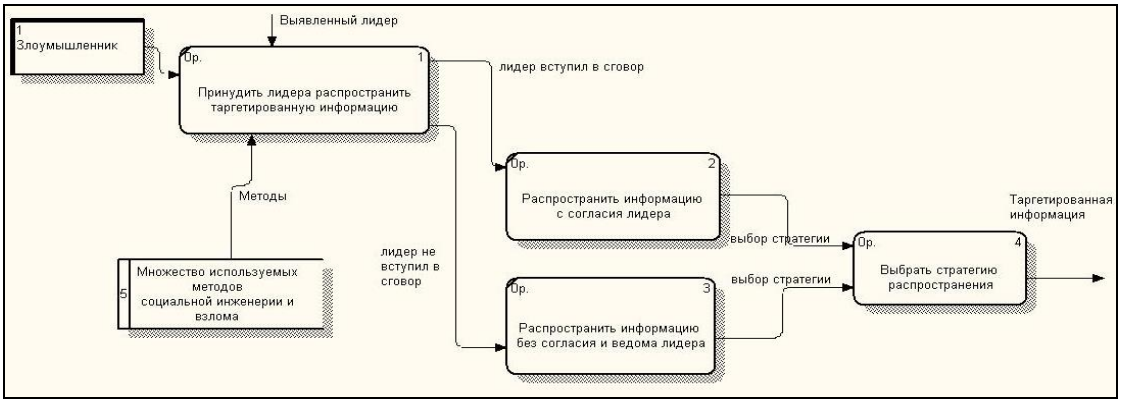

Рис.2.DFD диаграмма декомпозиции сценария распространения информации с помощью лидера социальной сети
Fig.2.DFD diagram of the decomposition of the information dissemination scenario with the help of the leader of the social network

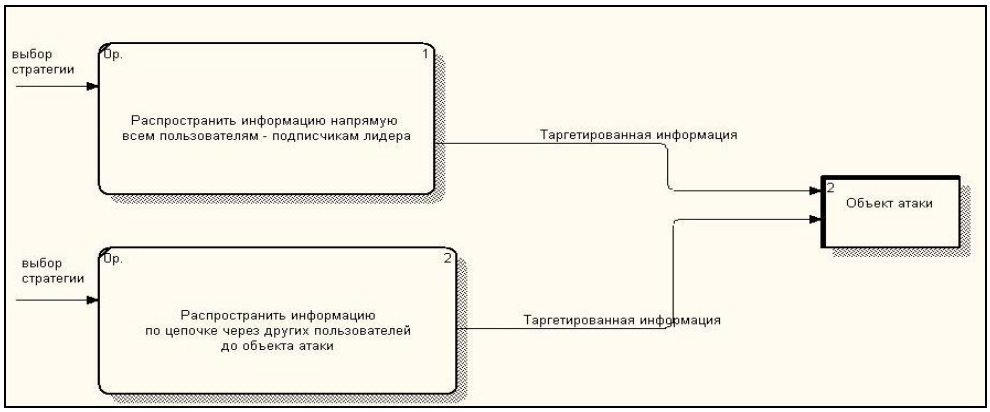

Рис.3.DFD диаграмма декомпозиции сценария выбора стратегии распространения информации в социальных сетях

Fig.3.DFD diagram of decomposition of the scenario of the choice of the strategy of distribution of information in social networks

На рисунках 2, 3 представлены следующие уровни декомпозиции «Распространить информацию с помощью лидера» (блок 3 рисунка 1), «Выбрать стратегию распространения» (блок 4 рисунка 2) соответственно.

В работе предложена методика защиты от распространения таргетированной информации в социальных сетях (рис. 4) представляет собой последовательность шагов:

1. Классификация пользователей социальной сети.
2. Защита лидеров социальной сети.
3. Совершенствование правил фильтрации сообщений пользователей.
4. Выработка рекомендаций по защите от распространения таргетированной информации [12 – 15].

Формально данную методику можно представить:

$K = \{k_1, k_2, k_3, k_4\}$ - множество функциональных блоков методики, где k_1 - классификация пользователей социальной сети, k_2 - защита лидеров социальной сети, k_3 - совершенствование правил фильтрации сообщений пользователей, k_4 - выработка рекомендаций по защите от распространения таргетированной информации;

$X = \{x_i \mid i = \overline{1,n}\}$ - множество входных параметров, где x_1 - образы злоумышленников, x_2 - критерии классификации потенциальных злоумышленников, x_3 - антивирусное программное обеспечение, x_4 - параметры пользователя-лидера социальной сети, x_5 - параметры, характеризующие поведение пользователя-лидера социальной сети, x_6 - множество сообщений пользователей, x_7 - критерии оценивания информации сообщений пользователей, x_8 - правила классификации информационных сообщений пользователей, x_9 - правила формирования рекомендаций по защите от таргетированной информации, x_{10} - множество пользователей социальной сети;

$Z = \{z_\varphi \mid \varphi = \overline{1,s}\}$ - множество внутренних параметров методики, где z_1 - перечень лидеров социальной сети, z_2 - информационные сообщения о необходимости соблюдения мер безопасности, z_3 - аутентификация с использованием технических средств связи, z_4 - профиль пользователя-лидера социальной сети, z_5 - база данных действий пользователя-лидера социальной сети, z_6 - принятие решений о блокировке аккаунта, z_7 - база данных сообщений таргетированной информации, z_8 - ожидаемые сообщения пользователя социальной сети, z_9 - нежелательные сообщения пользователя социальной сети;

$Y = \{y_j \mid j = \overline{1,m}\}$ - множество выходных параметров методики, где y_1 - перечень заблокированных пользователей, y_2 - информационное сообщение пользователю социальной сети о возможной реализации атаки, y_3 - рекомендации о принятии необходимых мер обеспечения информационной безопасности в социальной сети.

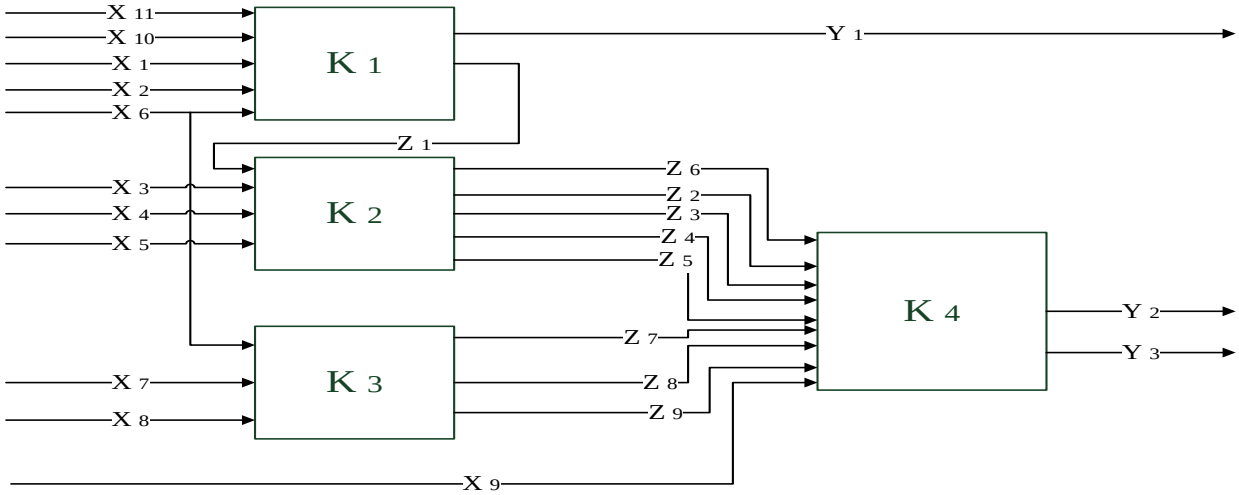

Рис.4. Структурная схема методики защиты от таргетированной информации
Fig.4. Structural scheme of the method of protection from the targeted information

Функциональный блок «Классификация пользователей социальной сети» включает:

1) классификацию пользователей на основе образов злоумышленников и выявление подозрительных пользователей – потенциальных злоумышленников;

2) классификацию потенциальных злоумышленников на основе критерия – уровень активности (действий) в отношении пользователей социальных сетей за определенное время t_1;

3) принятие решения о блокировании пользователей на основе п. 1 и п. 2 данного функционального блока;

4) классификация пользователей социальной сети на основе образов «пользователь-лидер социальной сети».

Функциональный блок «Защита лидеров социальной сети» включает:

1) обучение и предостережение лидеров сети – введение мер по обучению лидеров социальных сетей основам информационной безопасности (аккаунты лидеров являются критическими ресурсами, при получении доступа, к которым злоумышленник сможет распространить таргетированную информацию большому числу пользователей) путем рассылки информационных сообщений, содержащих напоминания о необходимости соблюдения мер информационной безопасности.

2) осуществление технических мер защиты: аутентификация с помощью смартфона (телефона), использование антивирусного программного обеспечения, аутентификация с помощью аппаратных средств, автоматическая проверка пароля на соответствие рекомендациям информационной безопасности.

3) анализ поведения лидера в социальной сети: разработка профиля пользователя (определение параметров пользователей и их граничных значений), создание базы данных действий пользователей, обновление базы данных действий пользователей, классификация поведения пользователя в социальной сети, разработка модели динамического изменения профиля пользователя, алгоритм определения аномального поведения пользователя.

В случае если поведение пользователя в сети является аномальным, то осуществляется информационное уведомление о том, что он является подозрительным с последующей блокировкой аккаунта.

На рисунке 5 представлена ER-диаграмма логической модели базы данных пользователей социальной сети.

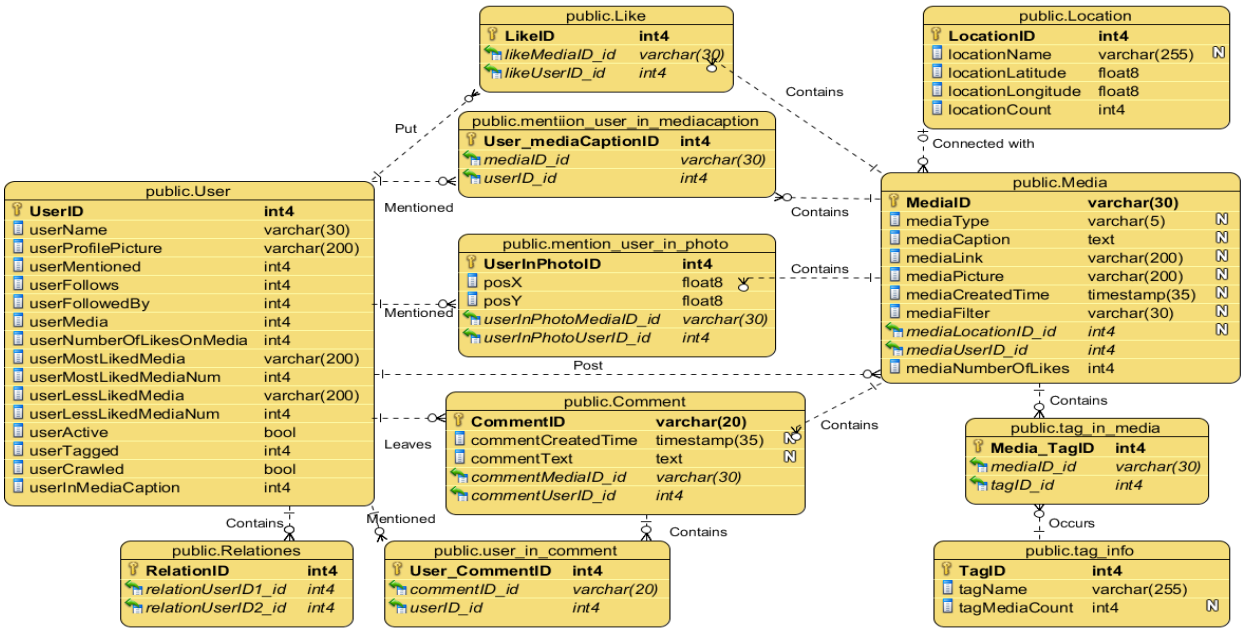

Рис.5. ER-диаграмма модели базы данных пользователей социальной сети
Fig.5. ER-diagram of the database model of social network users

Функциональный блок «Совершенствование правил фильтрации сообщений пользователей» декомпозируется на этапы:

- формирование базы данных сообщений пользователей, содержащих таргетированную информацию, распространяемую в социальных сетях на основе анализа данных заблокированных пользователей;
- разработка критериев оценивания информации сообщений пользователей;
- формирование базы правил классификации информации сообщений пользователей;
- детализация базы данных сообщений пользователей, содержащих таргетированную информацию, и их классификация на ожидаемые и нежелательные на основе критериев оценивания;
- совершенствование базы правил классификации;
- разработка модели фильтрации сообщений пользователей социальных сетей.

Функциональный блок «Выработка рекомендаций по защите от таргетированной информации» декомпозируется на этапы:

- формирование базы правил выработки рекомендаций по защите от таргетированной информации;
- информирование пользователя социальной сети о возможной реализации атаки;
- выработка рекомендаций о принятии необходимых мер обеспечения информационной безопасности.

Апробация предложенной методики осуществлялась на базе виртуальных социальных сетей: Twitter, Facebook, Instagram, ежемесячная аудитория пользователей которых составляет 310 млн., 900 млн., 100 млн. [16 – 21] соответственно. В эксперименте участвовало более 2000 пользователей данных социальных сетей. На рисунке 6 представлены статистические данные, полученные автором в результате исследования. До применения методики пользователи были заблокированы администраторами либо модераторами социальных сетей по причинам некорректных или нецензурных высказываний, подозрительного поведения в сообществах и т.п.

Стоит отметить, что доля заблокированных пользователей «безвозвратно» в общей массе заблокированных невелико (график 1, рис. 6). Статистические данные, полученные после применения методики показывают, что принятие решения о блокировании пользователей становится более взвешенной и количество заблокированных пользователей снижается, что подтверждается графиком 2 (рис. 6). Среднее значение заблокированных пользователей сократилось в 2,26 раза.

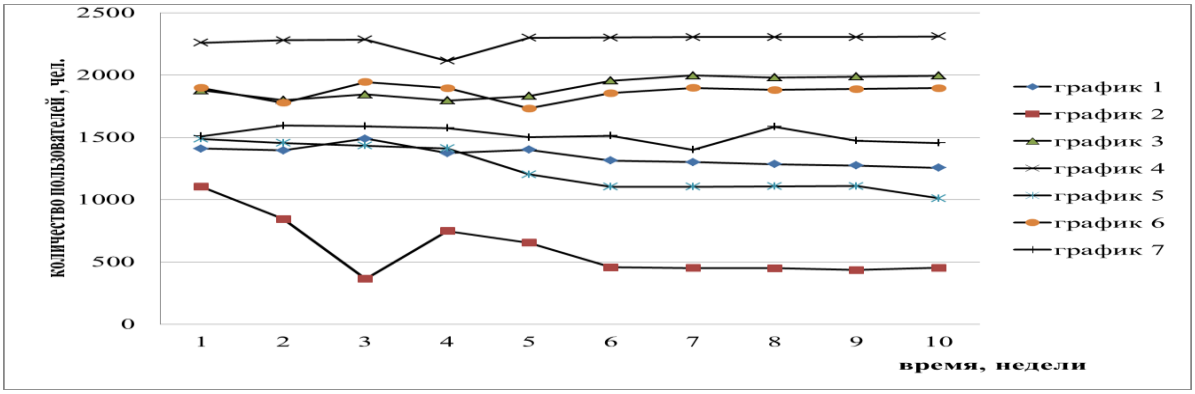

Рис.6. Статистические данные по апробации методики защиты от таргетированной информации

Fig.6. Statistical data on approbation of the method of protection against targeted information

Распространение злоумышленниками таргетированной информации пользователям социальных сетей осуществляется по причине реализации сценариев или части сценариев кибератак (график 3, рис. 6). Проще всего, как показывает статистика, злоумышленнику найти контакт с лидером сообщества и через него, используя методы социальной инженерии, распространить таргетированную информацию (график 4, рис. 6). Эффективность распространения таргетированной информации через лидера сообщества систем микроблоггинга составляет 1,19 раз. После применения методики защиты от таргетированной информации, путем реализации функционального блока «Защита лидеров социальной сети», выявлена динамика статистических данных. Пользователи социальных сетей отмечают (график 5, рис. 6), что стали реже (меньше на 35%) получать нежелательную информацию от друзей лидеров сообществ средствами микроблоггинга.

Зачастую злоумышленники используют стандартные типовые приемы для создания нежелательной информации в виде сообщений, дополняя их таргетированной информацией, например, ссылкой на вредоносное программное обеспечение. От качества и полноты базы данных правил классификации информации сообщений пользователей, содержащих таргетированную информацию зависит качество фильтрации сообщений и количество попыток блокирования нежелательных сообщений, содержащих таргетированную информацию (график 6, рис. 6). После применения методики количество пользователей, получивших нежелательные сообщения, содержащие таргетированную информацию сократилось на 19% (график 7, рис. 6).

Перспективы дальнейшего исследования проблемы защиты от таргетированной информации мы видим в детальной проработке методики и разработке на ее основе модели защиты от таргетированной информации. Модель защиты от таргетированной информации в социальных сетях позволит реализовать специальное программное обеспечение для его интегрирования в наиболее распространённые социальные сети, а пользователям повысить безопасность использования личной информации в социальных сетях и не попадаться на уловки злоумышленников. Предполагается, что специальное программное обеспечение будет представлять собой программный модуль – приложение, позволяющее: фильтровать личные сообщения пользователей, сообщений-записей (постов) пользователей сообществ социальных сетей на основе модели фильтрации сообщений; в автоматизированном режиме блокировать пользователей, рассылающих нежелательную информацию на основе образов злоумышленников, базы правил о блокировании пользователей; предоставлять рекомендации администраторам (модераторам) социальных сетей о возможных угрозах реализации атак злоумышленниками и принятии контрмер по предотвращению кибератак в социальных сетях. Исследования в этом направлении будут продолжены.

Вывод. Предложенная в работе методика защиты от таргетированной информации в социальных сетях, позволит предотвратить угрозы информационной безопасности, предотвратить попытки злоумышленников реализации социоинженерных атак, разработать

модель защиты от таргетированной информации, и в дальнейшем реализовать специальное программное обеспечение для его интегрирования в системы Online Social Network.

Все это позволит проводить внешний мониторинг событий в социальных сетях, а также осуществлять поиск уязвимостей в механизмах обмена мгновенными сообщениями для возможности реализации атак злоумышленниками, защите личной информации пользователей социальных сетей. Результаты исследования позволяют на новом уровне применять активно развивающийся сегодня сетевой подход к исследованию неформальных сообществ, получая интересные и наглядные результаты.

Библиографический список:

1. В. Левцов, Н. Демидов. Анатомия таргетированной атаки // Системный администратор. [Электронный ресурс] – http://samag.ru/archive/article/3170[Дата обращения: 06.03.2017].
2. Маркелова А.В., Козырева В.А., Сметанина О.Н. Модели управления процессом реализации академической мобильности в вузе // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2011. Т. 9. № 2. С. 55 – 65.
3. 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. Всборнике: Information Technologies for Intelligent Decision Making Support (ITIDS'2016) Proceedings of the 4th International Conference. 2016. С. 24 – 27.
4. 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.
5. Яшников А.Ю., Болодурина И.П. Выявление лидеров мнений социальной сети // Молодежный научный форум: технические и математические науки. 2016. № 5 (34). С. 59 – 65.
6. Мирзануров Д.Х.Методика защиты от нежелательной информации, распространяемой в системах SOCIAL NETWORK // Символ науки. 2015. № 5. С. 48 – 51.
7. Мирзануров Д.Х. Методика защиты от таргетированной информации, распространяемой в системах SOCIAL NETWORK // Приволжский научный вестник. 2015. № 6-1 (46). С. 40 – 43.
8. Е. Царев. Анатомия атаки в социальных сетях от Майка Рагго [Электронный ресурс] – http://www.tsarev.biz/informacionnaya-bezopasnost/anatomiya-ataki-v-socialnyx-setyax-ot-majka-raggo/[Дата обращения: 06.03.2017].
9. Служба внешней разведки штурмует соцсети [Электронный ресурс] – http://www.rbc.ru/society/27/08/2012/5703fbef9a7947ac81a6b1cd [Дата обращения: 06.03.2017].
10. Федоров П. ВКонтакте опережает Instagram по числу зарегистрированных пользователей [Электронный ресурс] – http://siliconrus.com/2014/01/vkontakte-operezhaet-instagram-po-chislu-zaregistrirovannyih-polzovateley/ [Дата обращения: 21.09.2016].
11. Юсупова Н.И., Шахмаметова Г.Р. Интеграция инновационных информационных технологий: теория и практика // Вестник Уфимского государственного авиационного технического университета. 2010. Т. 14. № 4 (39). С. 112 – 118.
12. 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.
13. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] – http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm [Дата обращения: 20.09.2016].

14. 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.
15. 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.
16. Майдыков А.А., Исаров О.Б. Национальные интересы - актуальные проблемы противодействия использованию интернета террористическими и экстремистскими организациями // Национальные интересы: приоритеты и безопасность. 2015. № 38 (323). С. 44 – 51.
17. Eset: аккаунты соцсетей 60% пользователей рунета взламывались хакерами [Электронный ресурс] – http://www.securitylab.ru/news/442581.php [Дата обращения: 21.09.2016].
18. А. Коршунов. Анализ данных пользователей социальных сетей [Электронный ресурс] – http://synthesis.ipi.ac.ru/sigmod/seminar/korshunov20130530.pdf [Дата обращения: 06.03.2017].
19. Д. Кремнёв. Продвижение в социальных сетях. [Электронный ресурс] – http://owlweb.ru/wp-content/uploads/2015/10/21681337d0ac6c287594c8fc8b5bb733.pdf [Дата обращения: 06.03.2017].
20. А. Коршунов, И. Белобородов, Н. Бузун, В. Аванесов, Р. Пастухов, К. Чихрадзе, И. Козлов, А. Гомзин, И. Андрианов, А. Сысоев, С. Ипатов, И. Филоненко, К. Чуприна, Д. Турдаков, С. Кузнецов. Анализ социальных сетей: методы и приложения. [Электр. ресурс] – http://www.ispras.ru/proceedings/docs/2014/26/1/isp_26_2014_1_439.pdf [Дата обращения 06.03.2017].
21. 15 самых популярных социальных сетей мира [Электронный ресурс] – https://ain.ua/2014/06/09/15-samyx-populyarnyx-socialnyx-setej-mira [Дата обращения: 06.03.2017].

References:

1. Levtsov V., Demidov N. Anatomiya targetirovannoy ataki . Sistemnyy administrator. [Elektronnyy resurs] – http://samag.ru/archive/article/3170 [Data obrashcheniya: 06.03.2017]. [Levtsov V., Demidov N. Anatomy of the targeted attack. System Administrator. [Electronic resource] – http://samag.ru/archive/article/3170 [Acces date: 06.03.2017]. (in Russ.)]
2. Markelova A.V., Kozyreva V.A., Smetanina O.N. Modeli upravleniya protsessom realizatsii akademicheskoy mobil'nosti v vuze. Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Informatsionnye tekhnologii. 2011; 9(2):55-65. [Markelova A.V., Kozyreva V.A., Smetanina O.N. Models of management of the process of academic mobility in the university. Novosibirsk State University Journal of Information Technologies. 2011; 9(2):55-65. (in Russ.)]
3. Yusupova N.I., Rizvanov D.A., Smetanina O.N., Enikeeva K.R. Modeli predstavleniya znaniy dlya podderzhki prinyatiya resheniy pri upravlenii slozhnymi sistemami v usloviyakh neopredelennosti i resursnykh ogranicheniy. Proceedings of the 4th International Conference “Information Technologies for Intelligent Decision Making Support (ITIDS'2016)”. Ufa; 2016. P. 24 – 27. [Yusupova N.I., Rizvanov D.A., Smetanina O.N., Enikeeva K.R. Knowledge representation models for decision support in managing complex systems under uncertainty and resource constraints. Proceedings of the 4th International Conference “Information Technologies for Intelligent Decision Making Support (ITIDS'2016)”. Ufa; 2016. P. 24 – 27. (in Russ.)]
4. Yusupova N.I., Smetanina O.N., Enikeeva K.R. Ierarkhicheskie situatsionnye modeli dlya SPPR v slozhnykh sistemakh. Sovremennye problemy nauki i obrazovaniya. 2013; 4:63-68. [Yusupova N.I., Smetanina O.N., Enikeeva K.R. Hierarchical situational models for DSS in complex systems. Modern problems of science and education. 2013; 4:63-68. (in Russ.)]
5. Yashnikov A.Yu., Bolodurina I.P. Vyyavlenie liderov mneniy sotsial'noy seti. Materialy XXXIV Studencheskoy mezhdunarodnoy zaochnoy nauchno-prakticheskoy konferentsii “Mo-

lodezhnyy nauchnyy forum: tekhnicheskie i matematicheskie nauki". 2016; 5(34):59-65. [Yashnikov A.Yu., Bolodurina I.P. Identifying the opinion leaders of the social network. Proceedings of XXXIV Student international correspondence scientific-practical conference "Molodezhnyy nauchnyy forum: tekhnicheskie i matematicheskie nauki". 2016; 5(34):59-65. (in Russ.)]

6. Mirzanurov D.H. Metodika zashchity ot nezhelatel'noy informatsii, rasprostranyaemoy v sistemakh SOCIAL NETWORK. Simvol nauki. 2015; 5:48-51. [Mirzanurov D.H. The method of protection against unwanted information distributed in SOCIAL NETWORK systems. Simvol nauki. 2015; 5:48-51. (in Russ.)]
7. Mirzanurov D.H. Metodika zashchity ot targetirovannoy informatsii, rasprostranyaemoy v sistemakh SOCIAL NETWORK. Privolzhskiy nauchnyy vestnik. 2015; 6-1(46): 40-43. [Mirzanurov D.H. The method of protection against the targeted information distributed in SOCIAL NETWORK systems. Privolzhskiy nauchnyy vestnik. 2015; 6-1(46): 40-43. (in Russ.)]
8. Tsarev E. Anatomiya ataki v sotsial'nykh setyakh ot Mayka Raggo [Elektronnyy resurs] – http://www.tsarev.biz/informacionnaya-bezopasnost/anatomiya-ataki-v-socialnyx-setyax-ot-majka-raggo/ [Data obrashcheniya: 06.03.2017]. [Tsarev E. Anatomy of the attack in social networks from Mike Ruggo [Electronic resource] – http://www.tsarev.biz/informacionnaya-bezopasnost/anatomiya-ataki-v-socialnyx-setyax-ot-majka-raggo/ [access date: 06.03.2017]. (in Russ.)]
9. Sluzhba vneshney razvedki shturmuet sotsseti [Elektronnyy resurs] – http://www.rbc.ru/society/27/08/2012/5703fbef9a7947ac81a6b1cd [Data obrashcheniya: 06.03.2017]. [The Foreign Intelligence Service is storming the social network [Electronic resource] – http://www.rbc.ru/society/27/08/2012/5703fbef9a7947ac81a6b1cd [access date: 06.03.2017]. (in Russ.)]
10. Fedorov P. VKontakte operezhaet Instagram po chislu zaregistrirovannykh pol'zovateley [Elektronnyy resurs] – http://siliconrus.com/2014/01/vkontakte-operezhaet-instagram-po-chislu-zaregistrirovannyih-polzovateley/ [Data obrashcheniya: 21.09.2016]. [Fedorov P. VKontakte ahead of Instagram by the number of registered users [Electronic resource] – http://siliconrus.com/2014/01/vkontakte-operezhaet-instagram-po-chislu-zaregistrirovannyih-polzovateley/ [access date: 21.09.2016]. (in Russ.)]
11. Yusupova N.I., Shakhmametova G.R. Integratsiya innovatsionnykh informatsionnykh tekhnologiy: teoriya i praktika. Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2010. 14-4(39):112-118. [Yusupova N.I., Shakhmametova G.R. Integration of innovative information technologies: theory and practice. Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2010. 14-4(39):112-118. (in Russ.)]
12. Nazarov A.N., Galushkin A.I., Sychev A.K. Risk-modeli i kriterii informatsionnogo protivoborstva v sotsial'nykh setyakh. T-Comm: Telekommunikatsii i transport. 2016; 10(7):81-86. [Nazarov A.N., Galushkin A.I., Sychev A.K. Risk-models and criteria of information confrontation in social networks. T-Comm. 2016; 10(7):81-86. (in Russ.)]
13. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii [Elektronnyy resurs] – http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm [Data obrashcheniya: 20.09.2016]. [The Doctrine of Information Security of the Russian Federation [Electronic resource] – http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm [access date: 20.09.2016]. (in Russ.)]
14. Tul'taeva I.V., Kaptyukhin R.V., Tul'taev T.A. Vozdeystvie sotsial'nykh setey na kommunikatsionnye protsessy v sovremennom obshchestve. Biznes. Obrazovanie. Pravo. Vestnik Volgogradskogo instituta biznesa. 2014; 4:84-88. [Tul'taeva I.V., Kaptyukhin R.V., Tul'taev T.A. The Impact of Social Networks on Communication Processes in Modern Society. Business. Education. Law. Bulletin of the Volgograd Business Institute. 2014; 4:84-88. (in Russ.)]
15. Murzin F.A., Batura T.V., Proskuryakov A.V. Programmnyy kompleks dlya analiza dannykh iz sotsial'nykh setey. Programmnye produkty i sistemy. 2015; 4:188-197. [Murzin F.A., Batura

T.V., Proskuryakov A.V. A software package for analysing data from social networks. Programmnye produkty i sistemy. 2015; 4:188-197. (in Russ.)]

16. Maydykov A.A., Isarov O.B. Natsional'nye interesy - aktual'nye problemy protivodeystviya ispol'zovaniyu interneta terroristicheskimi i ekstremistskimi organizatsiyami. Natsional'nye interesy: prioritety i bezopasnost'. 2015; (323):44-51. [Maydykov A.A., Isarov O.B. National interests - topical issues of countering the use of the Internet by terrorist and extremist organizations. National interests: priorities and security. 2015; (323):44-51. (in Russ.)]
17. Eset: akkaunty sotssetey 60% pol'zovateley runeta vzlamyvalis' khakerami [Elektronnyy resurs] – http://www.securitylab.ru/news/442581.php [Data obrashcheniya: 21.09.2016]. [Eset: accounts of social networks 60% of users of runet hacked by hackers [Electronic resource] – http://www.securitylab.ru/news/442581.php [access date: 21.09.2016]. (in Russ.)]
18. Korshunov A. Analiz dannykh pol'zovateley sotsial'nykh setey [Elektronnyy resurs] – http://synthesis.ipi.ac.ru/sigmod/seminar/korshunov20130530.pdf [Data obrashcheniya: 06.03.2017]. [Korshunov A. Analysis of data from users of social networks [Electronic resource] – http://synthesis.ipi.ac.ru/sigmod/seminar/korshunov20130530.pdf [access date: 06.03.2017]. (in Russ.)]
19. Kremnev D. Prodvizhenie v sotsial'nykh setyakh. [Elektronnyy resurs] – http://owlweb.ru/wp-content/uploads/2015/10/21681337d0ac6c287594c8fc8b5bb733.pdf [Data obrashcheniya: 06.03.2017]. [Kremnev D. Promotion in social networks. [Electronic resource] – http://owlweb.ru/wp-content/uploads/2015/10/21681337d0ac6c287594c8fc8b5bb733.pdf [access date: 06.03.2017]. (in Russ.)]
20. Korshunov A., Beloborodov I., Buzun N., Avanesov V., Pastukhov R., Chikhradze K., Kozlov I., Gomzin A., Andrianov I., Sysoev A., Ipatov S., Filonenko I., Chuprina K., Turdakov D., Kuznetsov S. Analiz sotsial'nykh setey: metody i prilozheniya. [Korshunov A., Beloborodov I., Buzun N., Avanesov V., Pastukhov R., Chikhradze K., Kozlov I., Gomzin A., Andrianov I., Sysoev A., Ipatov S., Filonenko I., Chuprina K., Turdakov D., Kuznetsov S. Analysis of social networks: methods and applications. [Electronic resource] – http://www.ispras.ru/proceedings/docs/2014/26/1/isp_26_2014_1_439.pdf [access date 06.03.2017]. (in Russ.)]
21. 15 samykh populyarnykh sotsial'nykh setey mira [Elektronnyy resurs] – https://ain.ua/2014/06/09/15-samyx-populyarnyx-socialnyx-setej-mira [Data obrashcheniya: 06.03.2017]. [15 most popular social networks in the world [Electronic resource] – https://ain.ua/2014/06/09/15-samyx-populyarnyx-socialnyx-setej-mira [access date: 06.03.2017]. (in Russ.)]

Сведения об авторе.

Тумбинская Марина Владимировна - кандидат технических наук, доцент кафедры систем информационной безопасности

Information about the author.

Marina V. Tumbinskaya – Cand. Sc.(Technical), Associate Prof. of Information Security Systems

Конфликт интересов **Conflict of interest**

Автор заявляет об отсутствии конфликта интересов. The author declare no conflict of interest.

Поступила в редакцию 19.01.2017. **Received** 19.01.2017.

Принята в печать 09.02.2017. **Accepted for publication** 09.02.2017.