http://vestnik.mrsu.ru
ISSN Print 0236-2910
ISSN Online 2313-0636

УДК 004.056.57:316.472.4 DOI: 10.15507/0236-2910.027.201702.264-288

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ОТ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

М. В. Тумбинская
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А. Н. Туполева»
(г. Казань, Россия)
tumbinskaya@inbox.ru

Введение. Социальные сети позволяют получить большой объем информации о пользователях. Этот процесс называется разведка на основе открытых источников. Пользователь социальных сетей самостоятельно предоставляет информацию о себе, публикуя данные о местах работы и учебы, косвенно рассказывает об интересах списком страниц и групп, в которых он состоит, публикуемыми записями и, таким образом, предоставляет сведения злоумышленникам, организующим целевые атаки на пользователей с помощью таргетированной информации.
Материалы и методы. В качестве объектов исследования были выбраны социальные сети Twitter, Facebook, ВКонтакте. Методами анализа и сравнения, а также путем моделирования были определены угрозы безопасности социальных сетей.
Результаты исследования. В работе формализован алгоритм распространения таргетированной информации в социальных сетях; определены его параметры, вариация которых позволит детализировать различные сценарии атак; предложена классификация угроз информационной безопасности, а также методика защиты от таргетированной информации, распространяемой в социальных сетях на основе исследования социальной информации.
Обсуждение и заключения. Перспективы дальнейшего исследования проблемы защиты от таргетированной информации мы видим в детальной проработке методики и разработке на ее основе модели защиты от таргетированной информации. Детализация сценариев атак позволит выработать меры противодействия. Методика защиты от таргетированной информации, распространяемой в социальных сетях, позволит разработать модель борьбы с такой информацией и реализовать специальное программное обеспечение для его интегрирования в социальных сетях.

Ключевые слова: информационная безопасность, социальная информационная система, таргетированная информация, злоумышленник, сценарий атаки

Для цитирования: Тумбинская М. В. Обеспечение защиты от нежелательной информации в социальных сетях // Вестник Мордовского университета. 2017. Т. 27, № 2. С. 264–288. DOI: 10.15507/0236-2910.027.201702.264-288

PROVIDING PROTECTION FROM TARGETED INFORMATION IN SOCIAL NETWORKS

M. V. Tumbinskaya
Tupolev Kazan National Research Technical University (Kazan, Russia)
tumbinskaya@inbox.ru

Introduction. Social networks provide massive information about users through the so-called open data mining. The social network users voluntarily disclose their personal information about their work, education, interests through pages and groups, which they join. Thus, important personal data become available for intruders, organizing network attacks against users through targeted information.
Materials and Methods. The social networks Twitter, Facebook, VKontakte are chosen as the objects of research. The methods of analysis, comparison and modeling identified threats to the security of social networks.
Results. The article formalizes the algorithm for the distribution of targeted information in social networks, defines its parameters, which allow detailing the various attack scenarios, and offers a classification of threats to information security. The technique of protection from targeted information in social networks is also offered.
Discussion and Conclusions. Detailing the scenarios of attacks allows developing countermeasures. The method of protection from the targeted information distributed in social networks allows developing a model of protection from targeted information and implementing special software for the integration into social networks.

***Keywords*:** information security, social information system, targeted information, the attacker, the attack scenario

For citation: Tumbinskaya M. V. Providing protection from targeted information in social networks. *Vestnik Mordovskogo universiteta* = Mordovia University Bulletin. 2017; 27(2):264-288. DOI: 10.15507/0236-2910.027.201702.264-288

Введение

В настоящее время большинство людей являются пользователями интернет-пространства, в котором активно развиваются виртуальные социальные сети – Online Social Network (OSN), или «микроблоггинг». OSN характеризуются простотой реализации продвижения бизнеса, распространения рекламы товаров и услуг, досуга, хобби, личного общения, обмена информацией и, таким образом, являются открытым источником информации для злоумышленников. Как правило, злоумышленники в OSN для достижения своих целей применяют мошеннические схемы, что подтверждается исследованиями [1–2].

В качестве одного из способов получения конфиденциальной информации они используют распространение таргетированной информации в OSN на основе методов манипуляции пользователями [3–4] и социальной инженерии. Под таргетированной информацией понимают нежелательную информацию, содержащуюся в информационных сообщениях пользователя или группы пользователей (сообщества) OSN.

Злоумышленники также могут использовать лидеров OSN (например, для вовлечения в террористические группировки [5–8]). Чаще всего лидеры имеют высокий уровень доверия среди большого количества пользователей; являются создателями (администраторами) сообществ.

Научная новизна работы заключается в формализации обобщенного алгоритма распространения таргетированной информации в OSN, который

положен в основу методики защиты от таргетированной информации, апробации предложенной методики на основе статистического исследования.

Обзор литературы

В результате анализа научной литературы было выявлено, что OSN в настоящее время находят широкое применение в различных сферах деятельности [9]. Обзор киберпреступников и кибермошенников представлен в работах [10–14]. Другие исследователи рассматривают различные способы мошенничества в наиболее распространенных OSN (Facebook, WhatsApp, Twitter и т. д.) и методы борьбы с ними [15–16].

Исследования, посвященные таргетированной рекламе в OSN, представлены в работах [18–20]. Вопросы распространения информациии в системах микроблоггинга поднимаются в исследованиях [21–22]. Модель поведения пользователей в системах микроблоггинга освещена в работе [22].

Вопросы доверия лидеру и информации, обрабатываемой в системах микроблоггинга, рассмотрены в статье [23]. Одной из целей злоумышленника при распространении таргетированной информации может быть конкурентная разведка, обзор способов которой представлен в исследованиях [24–26]. В настоящее время большое внимание уделяется защите информации в OSN. Например, в работах [27–31] рассмотрены основы информационной безопасности, способы потери данных, распространенных угрозах и уязвимостях OSN.

Материалы и методы

Рассмотрим примеры реализации кибератак злоумышленниками методами социальной инженерии в OSN, формализация которых представлена с применением методологии структурного анализа IDEF0. Функциональная модель (диаграмма A0) реализации кибератаки похищения денежных средств на основе методов социальной инженерии представлены на рис. 1. Данная кибератака подразумевает, что злоумышленник рассылает сообщение вредоносного содержания пользователю на электронную почту или в системе микроблоггинга. В случае успеха (т. е. если пользователь открывает сообщение вредоносного содержания) вирус заражает компьютер и похищает персональные данные.

На рис. 2 представлена диаграмма реализации кибератаки хищения конфиденциальных данных на основе метода социальной инженерии «кви про кво». Злоумышленник создает вредоносное программное обеспечение (ПО) под видом программы, повышающей быстродействие; осуществляет поиск заинтересованных пользователей на различных ресурсах и получает их контактные данные. Связывается с пользователями, убеждает их установить ПО и в случае успеха получает доступ к конфиденциальным данным.

На рис. 3 представлена диаграмма реализации кибератаки получения денежных средств методами социальной инженерии. Злоумышленником разрабатывается вредоносное ПО и отправляется сообщение, содержащее ссылку на него. Запуск программы позволяет злоумышленнику получить компрометирующую информацию, после чего он устанавливает связь с пользователем и средствами социальной инженерии вымогает денежные средства.

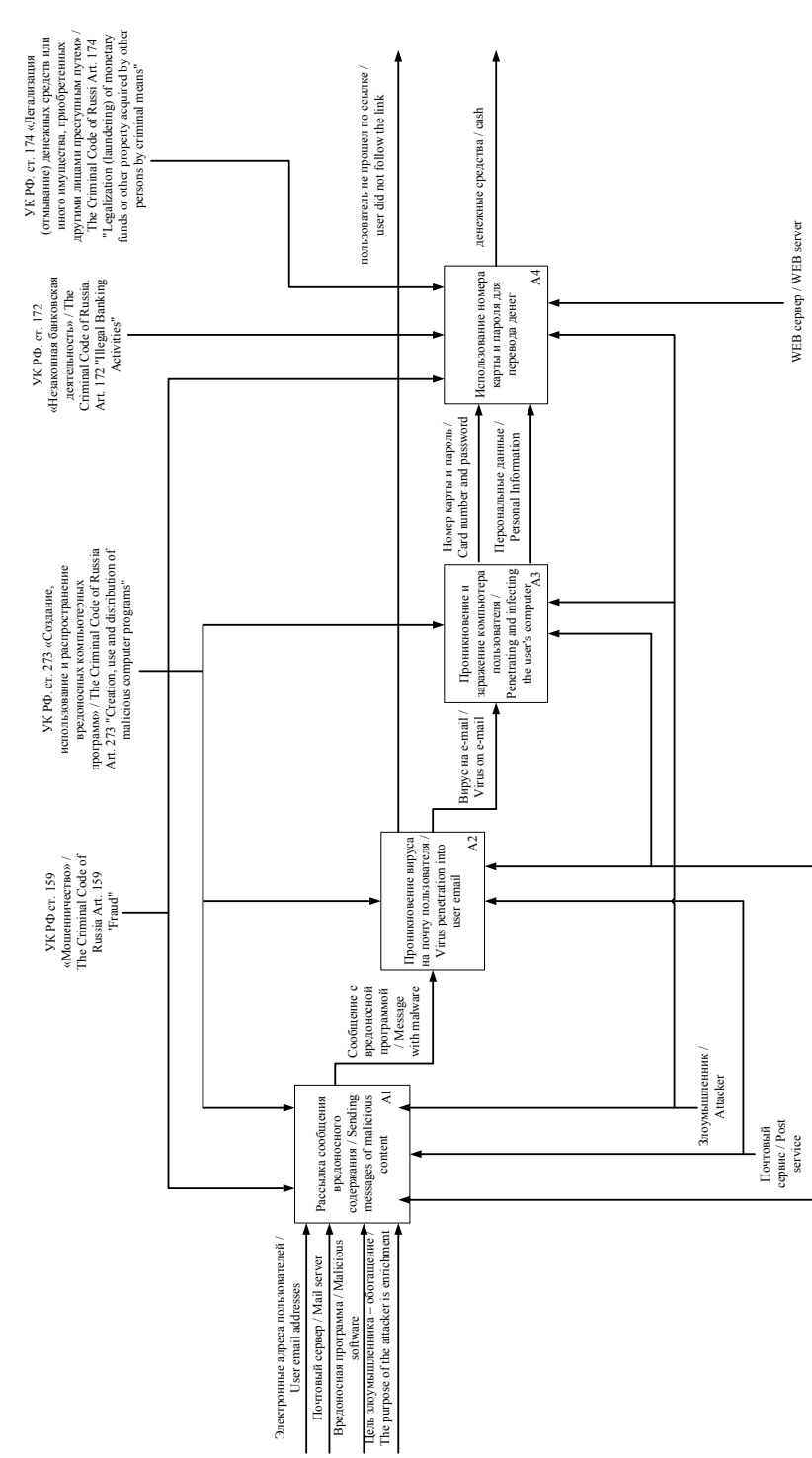

Рис. 1. Диаграмма А0 реализации кибератаки похищения денежных средств на основе методов социальной инженерии

Fig. 1. Diagram A0 of the implementating the cyberattack of stealing money based on the methods of social engineering

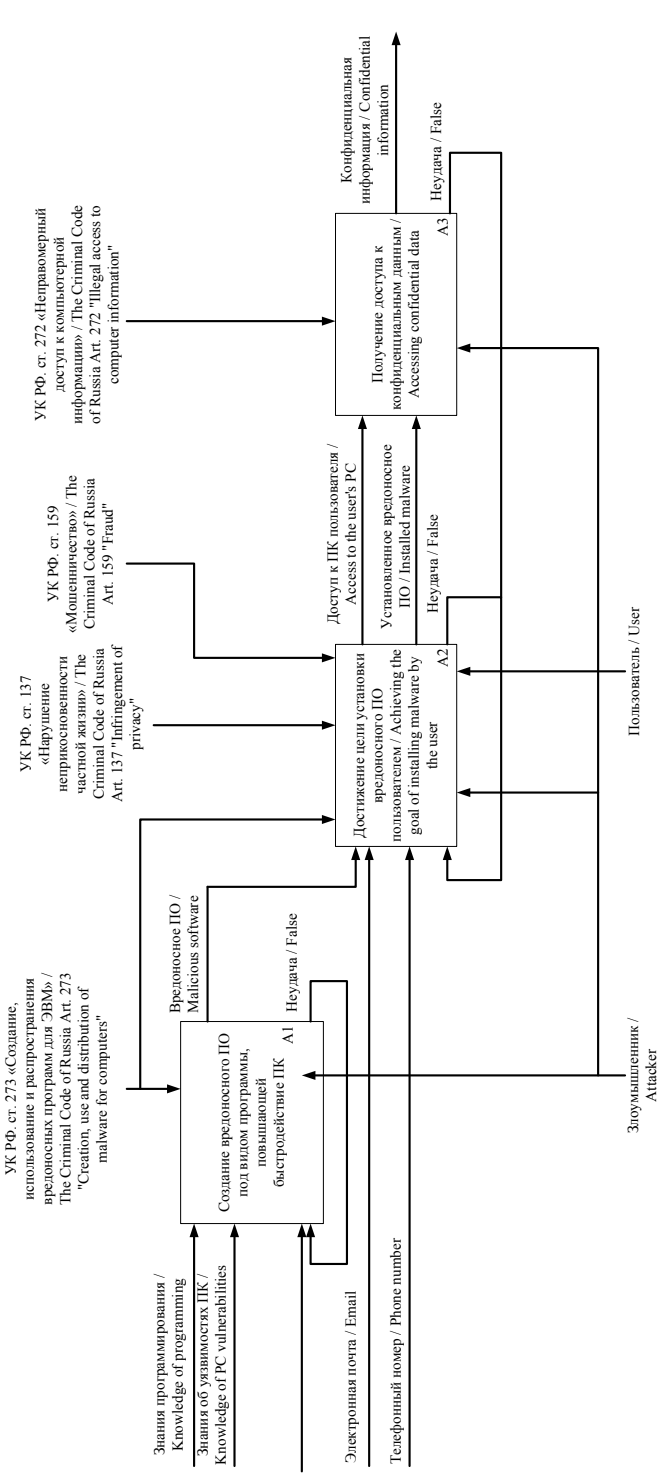

Рис. 2. Диаграмма A0 реализации кибератаки хищения конфиденциальных данных на основе метода социальной инженерии «кви про кво»
Fig. 2. Diagram A0 of the implementating of the cyber attack of stealing confidential data on the basis of the social engineering method "qui pro quo"

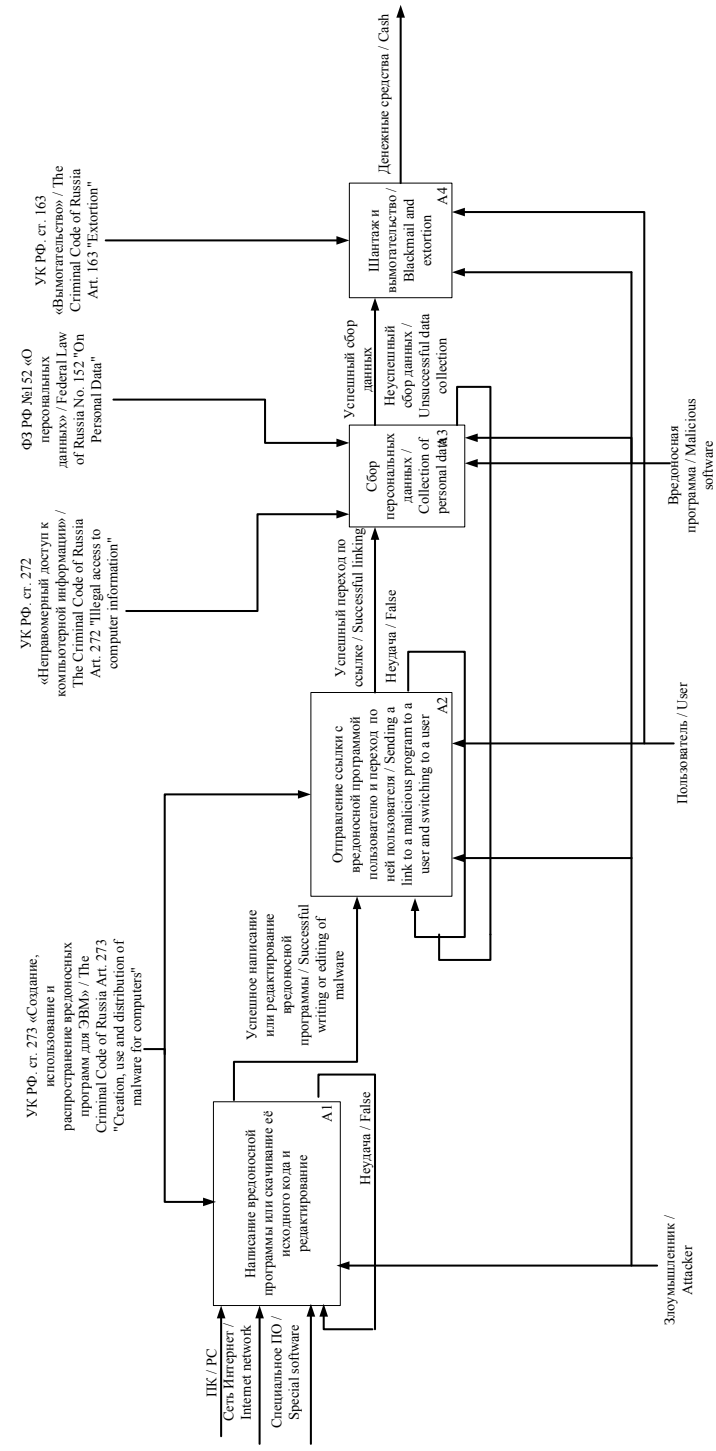

Рис. 3. Диаграмма A0 реализации кибератаки получения денежных средств методами социальной инженерии

Fig. 3. Diagram A0 of the implementating of the cyber attack of obtaining financial means by methods of social engineering

На основе анализа литературных источников [1–32] были выявлены основные уязвимости систем OSN:

1. Анализ сетевого трафика – исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей.

2. Сканирование сети – определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей.

3. Угроза выявления пароля – выполнение любого действия, связанного с получением несанкционированного доступа.

4. Подмена доверенного объекта сети – изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации.

5. Внедрение ложного объекта сети – перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации.

6. Отказ в обслуживании – частичное исчерпание ресурсов (снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений), исчерпание ресурсов (невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т. д.), нарушение логической связанности между атрибутами, данными, объектами (невозможность передачи сообщений из-за отсутствия корректных маршрутно-адресных данных). Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т. д., использование ошибок в программах (нарушение работоспособности сетевых устройств);

7. Удаленный запуск приложений – рассылка файлов, содержащих деструктивный исполняемый код, вирусное заражение (нарушение конфиденциальности, целостности, доступности информации), использование возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами (скрытое управление системой).

На рис. 4 представлена схема угроз в системах OSN. Модель угроз информационной безопасности должна определять:

– защищаемые объекты;

– основные угрозы безопасности информации, включая угрозы техногенного характера, стихийные бедствия и угрозы, реализуемые нарушителями;

– критерии уязвимости и устойчивости информационных систем к деструктивным воздействиям [33].

Обобщенный алгоритм распространения таргетированной информации в OSN

Предложенный алгоритм распространения был разработан на основе анализа работ [2–4; 29; 34–37].

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 OSN можно представить совокупностью исходных данных и результатов работы, которые позволят формализовать различные сценарии атак (табл. 1).

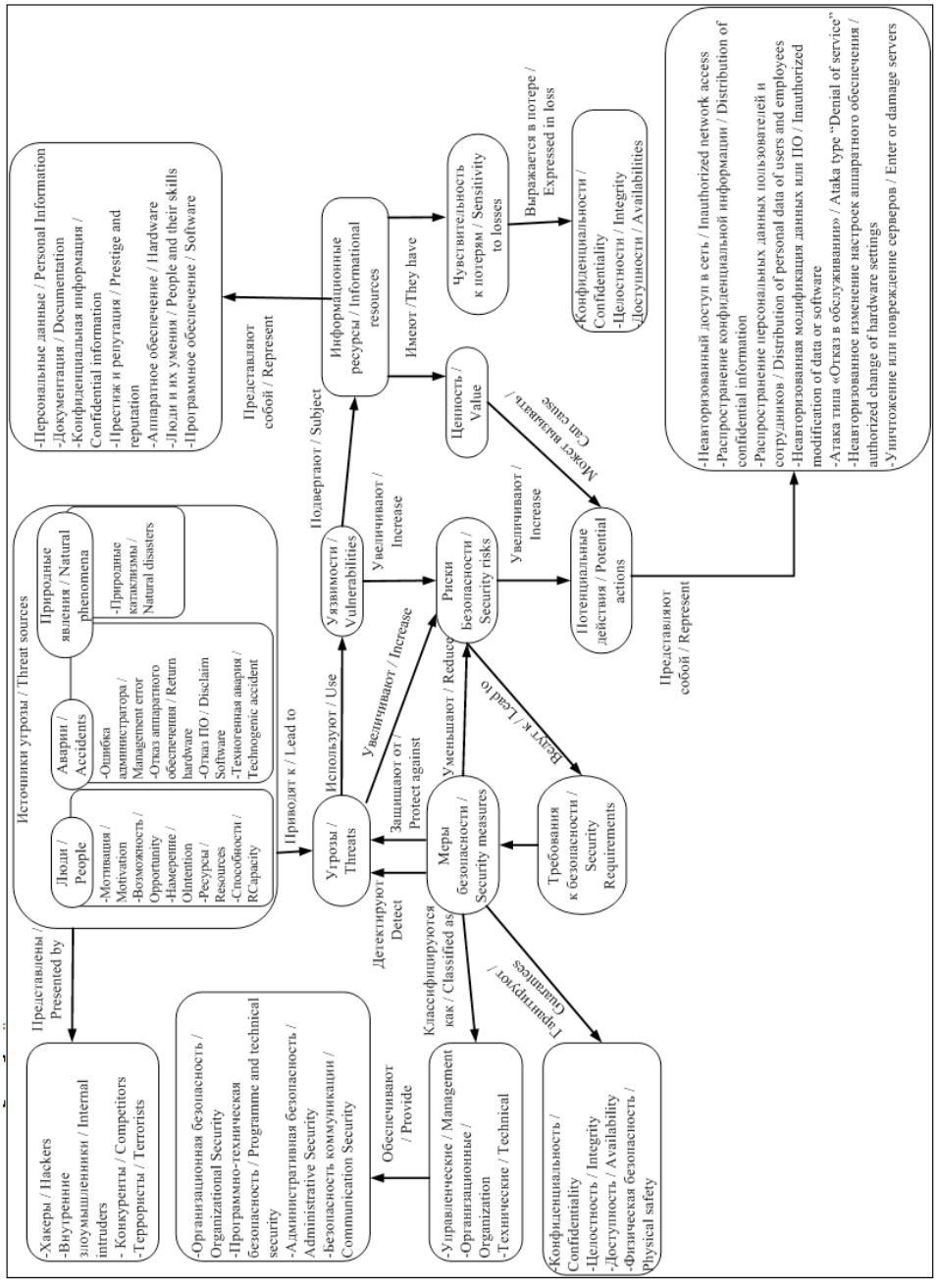

Рис. 4. Схема угроз в системах OSN
Fig. 4. Threat Scheme in OSN Systems

Таблица 1

Параметры обобщенного алгоритма распространения таргетированной информации в OSN

Вид группы параметров	Обозначение параметра	Интерпретация параметра
1	2	3
Входные параметры $X = \{x_1, ..., x_j\}$ – пользователи OSN	$x_1 = \{x_1^i \mid i = \overline{1,n}\}$ – идентификатор пользователя	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 OSN, образование, место проживания и т. д.)
	$x_2 = \{x_2^i \mid j = \overline{1,m}\}$ – посты пользователя социальной сети	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	x_3^1 – количество оценок других пользователей «мне нравится», x_3^2 – количество репостов сообщений другими пользователями сообществ, x_3^3 – количество сообщений в других OSN, x_3^4 – количество сообщений личного диалога пользователя
	$x_4 = \{x_4^\lambda \mid \lambda = \overline{1,\beta}\}$ – друзья и подписчики	x_4^1 – количество подписчиков пользователя, x_4^2 – количество друзей пользователя
	$x_5 = \{x_5^\sigma \mid \sigma = \overline{1,p}\}$ – профиль страницы пользователя	x_5^1 – закрытый профиль, x_5^2 – открытый профиль
	$x_6 = \{x_6^k \mid k = \overline{1,\tau}\}$ – посты	x_6^1 – количество постов пользователя, x_6^2 – ссылки на собственные сайты, другие OSN, x_6^3 – количество репостов
	$x_7 = \{x_7^d \mid d = \overline{1,w}\}$ – цель злоумышленника	x_7^1 – финансовая выгода, x_7^2 – самоутверждение перед самим собой, x_7^3 – самоутверждение перед лицом какого-либо сообщества/общества OSN, x_7^4 – возмездие знакомым пользователям, сообществу, мировой системе, x_7^5 – возмездие предприятию-работодателю, x_7^6 – преимущество в конкурентной борьбе, x_7^7 – удовлетворение хулиганских мотивов, x_7^8 – удовлетворение интереса, исследовательских целей

Продолжение табл. 1

1	2	3
Параметры внутренних состояний алгоритма $Z = \{z_1, ..., z_y\}$ – использование методов социальной инженерии пользователем OSN	$z_1 = \{z_1^i \mid i = \overline{1,k}\}$ – использование методов получения доступа к данным авторизации	z_1^1 – использование новых уязвимостей OSN 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 и ознакомление с файлами конфиденциальной информации путем использования доступа к сети организации, z_1^{14} – кража и 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	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 OSN под предлогом распространения благотворительной информации социальной направленности, z_2^8 – установление договоренностей с лидером OSN под предлогом распространения рекламной информации с последующим вознаграждением, z_2^9 – установление договоренностей с лидером OSN для распространения информации путем апелляции к иным скрытым мотивам (самоутверждение, обладание информацией)

Окончание табл. 1

1	2	3
	$z_3 = \left\{ z_3^\tau \mid \tau = \overline{1,\omega} \right\}$ – использование методов социальной инженерии, направленных на друзей лидера социальной сети	z_3^1 – использование методов получения доступа к данным авторизации ($z_1 = \left\{ z_1^i \mid i = \overline{1,k} \right\}$) для взлома друга лидера, z_3^2 – установление договоренностей с другом лидера OSN 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 OSN для распространения информации путем апелляции к иным скрытым мотивам (нематериальная выгода, самоутверждение, осведомленность)
Выходные параметры: $Y = \left\{ y_1, ..., y_p \right\}$ – 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	

T a b l e 1

Parameters of the generalized algorithm of the targeted information distribution in OSN

View of a group of parameters	Parameter designation	Parameter interpretation
1	2	3
Input parameters $X = \left\{ x_1, ..., x_j \right\}$ – OSN users	$x_1 = \left\{ x_1^i \mid i = \overline{1,n} \right\}$ – user ID	x_1^1 – graphical user image, x_1^2 – full name, x_1^3 – user's login, x_1^4 – age, x_1^5 – characteristics of the user (interests, belonging to social networking communities, education, place of residence, etc.)
	$x_2 = \left\{ x_2^j \mid j = \overline{1,m} \right\}$ – posts of the user of social network	x_2^1 – number of posts, x_2^2 – number of comments on posts, x_2^3 – geolocation of posts
	$x_3 = \left\{ x_3^\gamma \mid \gamma = \overline{1,s} \right\}$ – posts and messages assess	x_3^1 – number of likes, x_3^2 – number of messages from other community users, x_3^3 – number of messages in other social networks, x_3^4 – number of messages of the user's personal dialogue
	$x_4 = \left\{ x_4^\lambda \mid \lambda = \overline{1,\beta} \right\}$ – friends and subscribers	x_4^1 – number of subscribers, x_4^2 – number of friends

Table 1 continuation

1	2	3
	$x_5 = \left\{x_5^\sigma \mid \sigma = \overline{1, p}\right\}$ – user's profile	x_5^1 – closed profile, x_5^2 – open profile
	$x_6 = \left\{x_6^k \mid k = \overline{1, \tau}\right\}$ – posts	x_6^1 – number of posts, x_6^2 – links to own sites, other social networks, x_6^3 – number of reposts
	$x_7 = \left\{x_7^d \mid d = \overline{1, w}\right\}$ – target of attacker	x_7^1 – financial benefit, x_7^2 – self-assertion before oneself, x_7^3 – self-assertion in the face of any community/social network society, x_7^4 – revenge to familiar users, the community, the world system, x_7^5 – revenge to the employing enterprise, x_7^6 – advantage in competition, x_7^7 – hooliganism, x_7^8 – personal interest, research objectives
Parameters of the internal states of the algorithm $Z = \left\{z_1, ..., z_y\right\}$ – using the social engineering methods by OSN user	$z_1 = \left\{z_1^i \mid i = \overline{1, k}\right\}$ – using the methods for accessing authorization data	z_1^1 – using the new vulnerabilities of the social network and various data transfer protocols, z_1^2 – using the known vulnerabilities and data transfer protocols, z_1^3 – distribution of links to sites containing known malicious programs, z_1^4 – distribution of copies of known malware, z_1^5 – distribution of links to sites containing new self-described malicious programs, z_1^6 – distribution of copies of new malicious programs, z_1^7 – distribution of links to fishing sites, z_1^8 – using a direct attack, z_1^9 – using a dictionary attack, z_1^{10} – using a rainbow tables, z_1^{11} – hacking user account, z_1^{12} – hacking user's mailbox, z_1^{13} – theft and review of confidential information files by using access to the organization's network, z_1^{14} – theft and review of confidential information files by using physical access to the user's computer

End of table 1

	$z_2 = \left\{z_2^{\chi} \mid \chi = \overline{1,s}\right\}$ – using the social engineering techniques to gain access to authorization data	z_2^1 – using various pretexts for obtaining the password of personal acquaintances, z_2^2 – using a legend to retrieve a user password, z_2^3 – distribution of malicious software masquerading in the protection system, z_2^4 – using the infected physical media for obtaining passwords - Road apple, z_2^5 – using the trust relationship approach, z_2^6 – blackmail, z_2^7 – agreements with a leader of the social network under the pretext of distribution of charity social information, z_2^8 – agreement with a leader of a social network under the pretext of distributing advertising information with subsequent reward, z_2^9 – agreement with a leader of the OSN for the dissemination of information, appealing to other hidden motives (self-assertion, possession of information)
	$z_3 = \left\{z_3^{\tau} \mid \tau = \overline{1,\omega}\right\}$ – using the social engineering techniques aimed at the friends of the leader of the social network	z_3^1 – using the methods of access to authorization data ($z_1 = \left\{z_1^i \mid i = \overline{1,k}\right\}$) for hacking the leader's friend, z_3^2 – agreement with a friend of the OSN leader under the pretext of distributing charity social information, z_3^3 – agreement with a friend of the leader of the social network under the pretext of distributing advertising information with promises of reward to both the leader and a friend, z_3^4 – agreement with a friend of the leader of the OSN for the distribution of information, appealing to other hidden motives (non-material gain, self-affirmation, awareness)
Output parameters: $Y = \left\{y_1, ..., y_p\right\}$ – realized targets of attacker	y_1^1 – money, y_1^2 – self-assertion before oneself, y_1^3 – self-assertion in the face of community/society, y_1^4 – revenge to friends, y_1^5 – revenge to community, y_1^6 – revenge to world system, y_1^7 – revenge to employer, y_1^8 – advantage in competition, y_1^9 – hooliganism, y_1^{10} – interest	

Параметры $X = \left\{x_1,...,x_j\right\}$, представленные табл. 1, могут характеризовать одну из двух моделей потенциального нарушителя информационной безопасности OSN:

– пользователи, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в OSN, или нарушения функционирования OSN или обслуживающей ее инфраструктуры (преднамеренные угрозы);

– пользователи, непреднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы).

Целью моделирования нарушителя безопасности информации является формирование предположений о потенциальных возможностях реальных

нарушителей при реализации ими угроз в OSN. Модель нарушителя является частью модели угроз безопасности OSN и содержит:

– уровень физического доступа к информации в OSN;

– уровень логического доступа к информации в OSN;

– уровень компетенции нарушителя безопасности информации;

– уровень оснащенности нарушителя безопасности информации;

– мотивацию (цель) нарушителя безопасности информации [38].

В статье детализация внутренних состояний обобщенного алгоритма распространения таргетированной информации в OSN заложена в основу методики защиты от таргетированной информации.

Для разработки методики защиты от таргетированной информации необходимо выявить современное состояние информационного обмена в OSN. Для этого необходимо исследовать поведение пользователей в различных ситуациях, связанных с распространением таргетированной информации в OSN.

Обработка социальной информации в ситуациях распространения таргетированной информации в OSN

В исследовании приняли участие 2 499 пользователей социальных сетей Twitter, Facebook, ВКонтакте, являющихся модераторами (администраторами) сообществ пользователей Российской Федерации; возраст – от 17 до 30 лет. Все они участвовали в тестовом опросе, касающемся ситуаций распространения нежелательной информации в OSN и противодействия распространению таргетированной информации. Пользователи OSN участвуют в многочисленных ситуациях, связанных с распространением нежелательной информации как в роли жертвы, так и в роли потенциального злоумышленника. Благодаря этому они могут служить объектом изучения процесса принятия решения, фактов в ситуациях повышенного риска распространения нежелательной информации в OSN.

Анонимные тестовые опросы проводились в течение 6 месяцев в 2016–2017 гг. Один тестовый опрос пользователя длился ~ 1 ч. Опрос проводился с помощью тестовых бланков; результаты обрабатывались в статистическом пакете Statistica 10.0. Все респонденты дали добровольное письменное согласие на участие в исследовании.

Было изучено влияние обработки социальной информации, ситуационных и личностных параметров на повышение вероятности распространения нежелательной информации. Для этого была собрана информация от респондентов о ситуациях получения, распространения нежелательной информации и купирования тех, в которых они участвовали.

Ситуация получения таргетированной информации определяется как принудительное доведение потенциальным злоумышленником информационного сообщения средствами OSN и систем микроблоггинга до потенциальной жертвы для достижения своей цели. Ситуация распространения нежелательной информации предполагает массовую передачу потенциальным злоумышленником информационных сообщений пользователям OSN для достижения своей цели. Ситуация противодействия распространению нежелательной информации – это ситуация, в которой распространение информации, воспринимавшееся пользователем как возможное, не произошло по любой причине (например, блокировка подозрительного аккаунта, рассылающего спам).

Значения параметров тестового опроса представлены в бинарной шкале. Все параметры принимают значения либо «0», либо «1», что позволяет выявлять меры связи между ними. В соответствии с теорией обработки социальной информации (ТОСИ) проанализируем процесс принятия решения злоумышленником в ситуации распространения таргетированной информации. ТОСИ –

это социальный когнитивный подход, основанный на допущении, что человек «вступает в социальную ситуацию с набором биологически ограниченных возможностей и с базой данных о своем прошлом опыте» [39].

Средний возраст респондентов составил 22 года. Из них 74,99 % – мужчины, остальные – женщины. Более половины респондентов имеют законченное высшее образование (65,98 %). Большинство указали на принадлежность к низшему классу (70,99 %), поскольку респонденты являются студентами с основным источником доходов в виде стипендии и случайного заработка. Остальные респонденты относят себя к среднему классу (в 26 % случаев это магистранты и аспиранты, которые имеют возможность полноценно трудиться и заниматься наукой). 69,03 % респондентов не состоят в браке; 23,97 % имеют гражданского партнера; 7 % состоят в официальном браке. 81,03 % респондентов сообщили, что обладают средним уровнем знаний в IT-сфере, что объяснимо стремлением получить качественные знания в процессе обучения в вузе, а также возможностью совершения «безобидных» кибератак. Практически равномерным распределением процентного отношения респондентов к общему числу респондентов оказался параметр «принадлежность к социальной сети»: к группам OSN «хобби, развлечения» относится 21,93 %, «обучение» – 23,01 %, «религия» – 23,09 %, «знакомства» – 25,21 %, «бизнес» – 23,41 %, «проблема, беда» – 22,09 %.

Массовая популяризация основ информационной безопасности пользователей в OSN дает эффект фильтрации пользователем случайных аккаунтов в числе подписчиков и друзей: 39,98 % респондентов указали, что имеют < 50 аккаунтов-подписчиков, а 40,02 % – от 100 до 200 аккаунтов.

Респондентов сообщили о более чем 20 тыс. нежелательных сообщений, поступивших от различных пользователей OSN (табл. 2). За анализируемый промежуток времени 33,41 % пользователей получали от 4 до 10 сообщений, содержащих нежелательную информацию; 11,72 % отметили, что не получали подобные сообщения. В 39,98 % случаев отправителем сообщений, содержащих нежелательную информацию являются неизвестных пользователей; в 30,01 % – «фейковые» аккаунты. Реже всего такие сообщения приходят от друзей (5,00 %) и администраторов (модераторов) различных сообществ OSN (5,00 %). Данная статистика характеризуется тем, что друзья редко подвергают друг друга такого рода рассылкам, а администраторы (модераторы) сообществ дорожат своей репутацией.

Таблица 2

Table 2

Описательная статистика (за 6 месяцев) выборки из 2 499 пользователей о возможных ситуациях распространения таргетированной информации в социальных сетях

Descriptive statistics (for 6 months) sample of 2 499 users about possible situations of distribution of targeted information in social networks

Переменная / Variable	Частотность / Frequency	%
1	2	3
Количество получаемых сообщений нежелательного содержания / Number of unwanted content messages received		
не получал / did not receive	293	11,72
менее 3 раз / less than 3 times	732	29,29

Продолжение табл. 2 / Table 2 continuation

1	2	3
от 4 до 10 раз / from 4 to 10 times	835	33,41
от 11 до 15 раз / from 11 to 15 times	328	13,13
от 16 до 20 раз / from 16 to 20 times	210	8,40
более 20 раз / more than20 times	101	4,04
Отправитель сообщений нежелательного содержания / Who is the sender of unwanted messages in the social network?		
пользователи сообществ OSN / users of social network communities	500	20,01
модератор (администратор) OSN / Moderator (administrator) of the social network	125	5,00
фейковый аккаунт / fake account	750	30,01
друг / friend	125	5,00
неизвестный пользователь / unknown user	999	39,98
Содержание сообщений нежелательного содержания / Content of unwanted massages		
ссылка на вредоносный код / malicious code link	343	13,73
ссылка на фишинг сайт / link to fishing site	404	16,17
вовлечение в террористические группы / involvement in terrorist groups	362	14,49
вовлечение в сомнительные группы / involvement in suspicious groups	372	14,89
спам / spam	377	15,09
реклама товаров, услуг / advertising of goods and services	369	14,77
Количество кибератак на ваш аккаунт / Number of cyber attacks on the account		
нет / no	2 145	85,83
менее 3 раз / less than 3 times	353	14,13
от 4 до 10 раз / from 4 to 10 times	1	0,04
от 11 до 15 раз / from 11 to 15 times	0	0,00
более 15 раз / more than 15 times	0	0,00
Количество обращений в службу технической поддержки / Number of calls to technical support services		
не обращался / did not apply	1 994	79,79

Продолжение табл. 2 / Table 2 continuation

1	2	3
менее 5 раз / less than 5 times	266	10,64
от 5 до 20 раз / from 5 to 20 times	204	8,16
от 20 до 30 раз / from 20 to 30 times	35	1,40
от 30 до 50 раз / from 30 to 50 times	0	0,00
более 50 раз / more than 50 times	0	0,00
Количество обращений к модератору (администратору) OSN для блокировки определенного пользователя / Number of calls to the moderator (administrator) of the social network to block a specific user		
не обращался / did not apply	1 637	65,51
менее 5 раз / less than 5 times	676	27,05
от 5 до 20 раз / from 5 to 20 times	142	5,68
от 20 до 30 раз / from 20 to 30 times	0	0,00
от 30 до 50 раз / from 30 to 50 times	44	1,76
более 50 раз / more than 50 times	0	0,00
Сколько раз вам поступали предложения, как модератору (администратору) сообщества OSN сделать рассылку информационных сообщений нежелательного содержания пользователям вашего сообщества / How many times have you received suggestions, as a moderator (administrator) of the social network community, to send out information messages with unwanted content to users in your community?		
не поступали / did not arrive	337	13,49
менее 5 раз / less than 5 times	980	39,22
от 5 до 20 раз / from 5 to 20 times	690	27,61
от 20 до 30 раз / from 20 to 30 times	152	6,08
от 30 до 50 раз / from 30 to 50 times	171	6,84
более 50 раз / more than 50 times	169	6,76
Достигли ли вы своей цели путем распространения нежелательной информации, согласившись на рассылку информационных сообщений / Did you achieve your goal through disseminating unwanted information by agreeing to send out information messages?		
да / yes	1 646	65,87
нет / no	516	20,65
Количество обращений в службу технической поддержки с просьбой заблокировать аккаунт пользователя, распространяющего нежелательную информацию / How many times have you contacted the technical support service to block the user account that is distributing unwanted information?		
не обращался / did not apply	250	10,00

Окончание табл. 2 / End of table 2

1	2	3
менее 5 раз / less than 5 times	874	34,97
от 5 до 20 раз / from 5 to 20 times	1 000	40,02
от 20 до 30 раз / from 20 to 30 times	250	10,00
более 30 раз / more than 30 times	125	5,00
Количество ключевых словосочетаний/слов в базе данных сообщества (где вы являетесь модератором) для фильтрации сообщений / How many key phrases / words in the community database (where you are a moderator) for message filtering?		
менее 10 / less than 10	250	77,01
от 10 до 15 / from 10 to 15	249	9,96
от 15 до 20 / from 15 to 20	500	10,01
более 20 / more than 20	1 500	3,02

Респонденты отметили наличие всех предложенных вариантов содержания нежелательных сообщений (в приблизительно равном соотношении: 15±1 %). Это вредоносные программы, ссылки на фишинг-сайты, вербовка в террористические группировки, вовлечение в сомнительные группы, спам, реклама товаров и услуг. 85,83 % респондентов отметили отсутствие кибератак на их аккаунты и, следовательно, обращений в службу технической поддержки (79,79 %). Вероятнее всего, это обусловлено недостаточным промежутком времени исходной выборки (6 месяцев).

Пользователи OSN часто просят друг друга помочь в рассылке какой-либо информации (например, призыва о помощи). По статистике, большинству респондентов сообщения подобного рода поступали < 5 раз (39,22 %) или не поступали вовсе (13,49 %). Соглашаясь на рассылку таких сообщений, многие респонденты преследуют финансовую выгоду (71,67 %) или цель самоутвердиться (54,94 %). 65,87 % респондентов отметили, что достигли своих целей средствами рассылки информации нежелательного содержания. Рассылку таргетированной информации можно предотвратить путем фильтрации информационных сообщений пользователей OSN. Так 77,01 % респондентов отметили, что ключевых словосочетаний/слов в базе данных фильтрации сообщений составляет < 10. Кроме того, следует учитывать семантику ключевых словосочетаний/слов для фильтрации сообщений.

Согласно результатам исследования, потенциальный злоумышленник может использовать различные способы распространения нежелательной информации в зависимости от поставленных целей. Самыми простыми и краткосрочными являются принуждение и привлечение администраторов (модераторов) сообществ в OSN, поскольку они чаще всего обладают высоким уровнем доверия среди пользователей и вероятность достижения своих целей злоумышленником в данном случае высока.

Результаты исследования

На основе исследования социальной информации в ситуациях распространения таргетированной информации в OSN в статье предложена методика защиты от распространения таргетированной информации в OSN (рис. 5), которая представляет собой последовательность шагов:

1. Классификация пользователей OSN.
2. Защита лидеров OSN.
3. Совершенствование правил фильтрации сообщений пользователей.
4. Выработка рекомендаций по защите от распространения таргетированной информации в OSN.

Формально данную методику можно представить в следующем виде:

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

$\tilde{O} = \{x_i \mid i = \overline{1,n}\}$ – множество входных параметров, где x_1 – образы злоумышленников; x_2 – критерии классификации потенциальных злоумышленников; x_3 – антивирусное ПО; x_4 – параметры пользователя-лидера OSN; x_5 – параметры, характеризующие поведение пользователя-лидера OSN; 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_0 – множество пользователей OSN.

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

$Y = \{y_j \mid j = \overline{1,m}\}$ – множество выходных параметров методики, где y_1 – заблокированные пользователи; y_2 – информационное сообщение о возможной реализации атаки; y_3 – рекомендации о принятии необходимых мер обеспечения информационной безопасности.

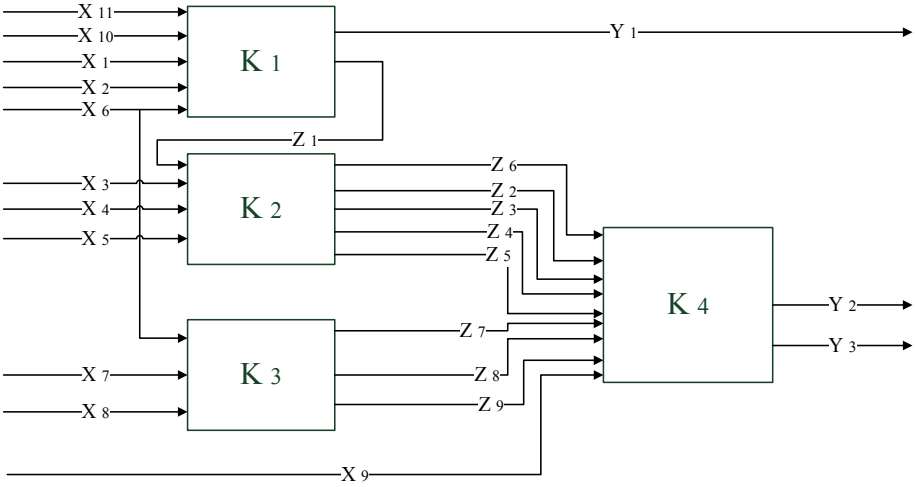

Рис. 5. Структурная схема методики защиты от таргетированной информации
Fig. 5. Structural diagram of the method for protection against targeted information

Функциональный блок «Классификация пользователей OSN» включает:

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

2) классификацию потенциальных злоумышленников на основе уровня активности (действий) в отношении пользователей OSN за определенное время t_1;

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

4) классификацию пользователей OSN на основе образов «пользователь-лидер OSN».

Функциональный блок «Защита лидеров OSN» включает:

1) обучение и предостережение лидеров сети – введение мер по обучению лидеров OSN основам информационной безопасности (аккаунты лидеров являются критическими ресурсами, при получении доступа к которым злоумышленник сможет распространить таргетированную информацию большому количеству 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 ПО, аутентификация с помощью аппаратных средств, автоматическая проверка пароля на соответствие рекомендациям информационной безопасности;

3) анализ поведения лидера в OSN: разработка профиля пользователя (определение параметров пользователей и их граничных значений), создание базы данных действий пользователей с последующим обновлением, классификация поведения пользователя в OSN, разработка модели динамического изменения профиля пользователя и алгоритма 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.

Функциональный блок «Совершенствование правил фильтрации сообщений пользователей» включает этапы:

1) формирование базы данных сообщений пользователей, содержащих таргетированную информацию, распространяемую в OSN на основе анализа данных заблокированных пользователей;

2) разработка критериев оценивания информации сообщений пользователей;

3) формирование базы правил классификации информации сообщений пользователей;

4) детализация базы данных сообщений пользователей, содержащих таргетированную информацию, и их классификация на ожидаемые и нежелательные на основе критериев оценивания;

5) совершенствование базы правил классификации;

6) разработка модели фильтрации сообщений пользователей OSN.

Функциональный блок «Выработка рекомендаций по защите от таргетированной информации в OSN»:

1) формирование базы правил выработки рекомендаций по защите от таргетированной информации;

2) информирование пользователя OSN о возможной реализации атаки (вероятность реализации);

3) выработка рекомендаций о принятии необходимых мер обеспечения информационной безопасности.

Обсуждение и заключения

Перспективы дальнейшего исследования проблемы защиты от таргетированной информации мы видим в детальной проработке методики и разработке на ее основе модели защиты от таргетированной информа-

ции. Модель защиты от таргетированной информации в OSN позволит реализовать специальное ПО для его интегрирования в наиболее распространенные OSN, а пользователям – повысить безопасность использования личной информации в OSN и не попадаться на уловки злоумышленников. Предполагается, что специальное ПО будет представлять собой программный модуль – приложение, позволяющее:

– фильтровать личные сообщения пользователей, сообщений-записей (постов) пользователей сообществ OSN 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) OSN о возможных угрозах реализации атак злоумышленниками и принятии контрмер по предотвращению кибератак в OSN.

Все это позволит проводить внешний мониторинг событий в OSN, а также осуществлять поиск уязвимостей в механизмах обмена мгновенными сообщениями для возможности реализации атак злоумышленниками, защите личной информации пользователей OSN. Результаты исследования позволяют на новом уровне применить активно развивающийся в настоящее время сетевой подход к исследованию неформальных сообществ.

Исследования в данном направлении будут продолжены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. **Bradbury D.** Spreading fear on facebook // Network security. 2012. Vol. 10. P. 15–17. URL: http://www.sciencedirect.com/science/article/pii/S1353485812700946

2. **Kim Hak J.** Online social media networking and assessing its security risks // International journal of security and its applications. 2012. Vol. 6, no. 3. P. 11–18. URL: http://s3.amazonaws.com/academia.edu.documents/32964814/onl_ine_sns.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1492687149&Signature=B %2FAeIWq4LJCG61nlkV3Ihi9Beis %3D&response-content-disposition=inline %3B %20filename %3DOnline_Social_Media_Networking_and_Asses.pdf

3. Advanced social engineering attacks / K. Krombholz [et al.] // Journal of information security and applications. 2014. Vol. 22. P. 1–10. URL: http://www.sciencedirect.com/science/article/pii/S2214212614001343

4. **Fire M., Goldschmidt R., Elovici Y.** Online Social Networks: threats and solutions // Journal of latex class files. 2012. Vol. 16, no. 4. P. 1–19. URL: http://ieeexplore.ieee.org/abstract/document/6809839/?reload=true

5. **Coppock V.** Can you spot a terrorist in your classroom? Problematising the recruitment of schools to the «War on Terror» in the United Kingdom // Global Studies of Childhood. 2014. Vol. 4, no. 2. P. 115–125. DOI: http://dx.doi.org/10.2304/gsch.2014.4.2.115

6. **Ennaji M.** Recruitment of foreign male and female fighters to Jihad: Morocco's multifaceted counter-terror strategy // International Review of Sociology. 2016. Vol. 26, no. 3. P. 546–557. DOI: http://dx.doi.org/10.1080/03906701.2016.1244954

7. **Klein G. R.** Ideology isn't everything: transnational terrorism, recruitment incentives, and attack casualties. // Terrorism and Political Violence. 2016. Vol. 26, no. 5 P. 868–887. DOI: http://dx.doi.org/10.1080/09546553.2014.961635

8. **Mahood S.**, **Rane H.** Islamist narratives in ISIS recruitment propaganda. // The Journal of International Communication. 2017. Vol. 23, no. 1. P. 1–21. DOI: http://dx.doi.org/10.1080/13216597.2016.1263231

9. **Rodriguez A. B., Garcia J. S.** Social networks in 20 minutos, the one survivor of free distribution press in Spain // Media and Metamedia Management. 2017. P. 429–434. DOI: http://dx.doi.org/10.1007/978-3-319-46068-0_56

10. **Akbari A., Mousavi S. M. A.** Criminological analysis of fraud in cyberspace // International journal of humanities and cultural studies. 2016. Special April. P. 56–64. URL: https://www.ijhcs.com/index.php/ijhcs/article/view/543

11. **Fedushko S., Bardyn N.** Algorithm of the cyber criminals identification // Global journal of engineering, design & technology. 2013. Vol. 4, no. 2. P. 56–62. URL: https://www.researchgate.net/profile/Solomia_Fedushko/publication/287646809_Algorithm_of_the_cyber_criminals_identification/links/56787f5e08ae502c99d5727e.pdf

12. **Nash R., Bouchard M., Malm A.** Investing in people: the role of social networks in the diffusion of a large-scale fraud // Social networks. 2013. Vol. 35, no. 4. P. 686–698. URL: http://www.sciencedirect.com/science/article/pii/S0378873313000567

13. Cybercrime and cybercriminals: a comprehensive study / R. Sabillon [et al.] // International journal of computer networks and communications security. 2016. Vol. 6, no. 4. P. 165–176. URL: http://www.ijcncs.org/published/volume4/issue6/p1_4-6.pdf

14. **Yosefi Z., Ahmadi A.** Investigating computer fraud in criminal justice system of iran // Cumhuriyet science journal. 2015. Vol. 36, no. 3. P. 3556–3565. URL: http://dergi.cumhuriyet.edu.tr/cumuscij/article/view/5000130788

15. Online frauds: learning from victims why they fall for these scams / M. Button [et al.] // Australian & New Zealand journal of criminology. 2014. Vol. 47, no. 3. P. 391–408. DOI: http://dx.doi.org/10.1177/0004865814521224

16. Anomaly detection in online social networks / D. Savage [et al.] // Social networks. 2014. Vol. 39. P. 62–70. URL: http://www.sciencedirect.com/science/article/pii/S0378873314000331

17. **Terlutter R., Capella M. L.** The gamification of advertising: analysis and research directions of in-game advertising // Advergames, and Advertising in Social Network Games, The Gamification of Advertising. 2013. Vol. 42, no. 2-3. P. 95–112. DOI: http://dx.doi.org/10.1080/00913367.2013.774610

18. Entertainment matters! The relationship between challenge and persuasiveness of an advergame for children / K. J. Martin [et al.] // Journal of Marketing Communications. 2012. Vol. 18. P. 69–89. URL: http://sci-hub.cc/10.1080/13527266.2011.620766

19. **Li S., Peitz M., Zhao X.** Information disclosure and consumer awareness // Journal of Economic Behavior & Organization. 2016. Vol. 128. P. 209–230. URL: http://www.sciencedirect.com/science/article/pii/S0167268116300804

20. **Johnson J. P.** Targeted advertising and advertising avoidance // Journal of Economics. 2013. Vol. 44, no. 1. P. 128–144. DOI: http://dx.doi.org/10.1111/1756-2171.12014/full

21. Microblog sentiment orientation detection using user interactive relationship / L. Wang [et al.] // Journal of Electrical and Computer Engineering. 2016. P. 167–181. DOI: http://dx.doi.org/10.1155/2016/7282913

22. Model study of information dissemination in microblog community networks / L. Wang [et al.] // Discrete Dynamics in Nature and Society. 2016. P. 331–354. URL: https://www.hindawi.com/journals/ddns/2016/8393016/abs

23. **Pellissier R., Tshilidzi E. Nenzhelele.** Towards a universal competitive intelligence process model: original research // South African Journal of Information Management. 2013. Vol. 15, no. 2. P. 1–7. URL: http://www.sajim.co.za/index.php/SAJIM/article/view/567

24. Actionable social media competitive analytics for understanding customer experiences / W. He [et al.] // Journal of Computer Information Systems. 2016. Vol. 56, no. 2. P. 145–155. DOI: http://dx.doi.org/10.1080/08874417.2016.1117377

25. **Trong Tuan Luu.** Competitive intelligence and other levers of brand performance // Journal of strategic marketing. 2013. Vol. 21, no 3. P. 217–239. DOI: http://dx.doi.org/10.1080/0965254X.2013.765501

26. **Trong Tuan Luu.** Organizational social capital as a moderator for the effect of entrepreneurial orientation on competitive intelligence. // Journal of Strategic Marketing. 2015. Vol. 25, no. 4. P. 1–15. DOI: http://dx.doi.org/10.1080/0965254X.2015.1076884

27. **Tucker C. E.** Social networks, personalized advertising, and privacy controls // Journal of Marketing Research. 2014. Vol. 51, no. 5. P. 546–562. DOI: http://dx.doi.org/10.1509/jmr.10.0355

28. **Najaflou Y., Jedari B., Xia F.** Safety Challenges and Solutions in Mobile Social Networks // IEEE Systems Journal. 2015. Vol. 9, no. 3. P. 834–854. URL: http://ieeexplore.ieee.org/abstract/document/6642041

29. **Fire M., Goldschmidt R., Elovici Y.** Online social networks: threats and solutions // IEEE Communications Surveys & Tutorials. 2014. Vol. 16, no. 4. P. 2019–2036. URL: http://ieeexplore.ieee.org/abstract/document/6809839

30. **Young A. L., Quan-Haase A.** Privacy protection strategies on Facebook // Information, Communication & Society. 2013. Vol. 16, no. 4. P. 479–500. DOI: http://dx.doi.org/10.1080/1369118X.2013.777757

31. **Heatherly R., Kantarcioglu M., Thuraisingham B.** Preventing private information inference attacks on social networks // IEEE Transactions on Knowledge and Data Engineering. 2013. Vol. 25, no. 8. P. 1849–1862. URL: https://pdfs.semanticscholar.org/829c/bf93318b1e2917740b8d368f85fb922ba97f.pdf

32. **Тультаева И. В., Каптюхин Р. В., Тультаев Т. А.** Воздействие OSN на коммуникационные процессы в современном обществе // Вестник Волгоградского института бизнеса. 2014. № 4. С. 84–88. URL: http://vestnik.volbi.ru/upload/numbers/429/article-429-970.pdf

33. **Назаров А. Н., Галушкин А. И., Сычев А. К.** Риск-модели и критерии информационного противоборства в OSN // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10, № 7. С. 81–86. URL: http://elibrary.ru/item.asp?id=26528114

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

35. Eset: аккаунты соцсетей 60 % пользователей рунета взламывались хакерами [Электронный ресурс]. URL: http://www.securitylab.ru/news/442581.php

36. Эмпирическая проверка теории обработки социальной информации и влияние эмоций в ситуациях насилия / К. Н. Боуэн [и др.] // Актуальные проблемы экономики и права. 2017. № 1. С. 189–207. URL: http://cyberleninka.ru/article/n/empiricheskaya-proverka-teorii-obrabotki-sotsialnoy-informatsii-i-vliyanie-emotsiy-v-situatsiyah-nasiliya

Поступила 15.03.2017; принята к публикации 24.04.2017; опубликована онлайн 14.06.2017

Об авторе:

Тумбинская Марина Владимировна, доцент кафедры систем информационной безопасности, Институт компьютерных технологий и защиты информации, ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А. Н. Туполева» (Россия, г. Казань 420111, ул. К. Маркса, д. 10), кандидат технических наук, **ORCID: http://orcid.org/0000-0003-3738-5242**, tumbinskaya@inbox.ru

Автор прочитала и одобрила окончательный вариант рукописи.

REFERENCES

1. Bradbury D. Spreading fear on facebook. Network security. 2012; 10:15-17. Available at: http://www.sciencedirect.com/science/article/pii/S1353485812700946

2. Kim Hak J. Online social media networking and assessing its security risks. International Journal of Security and its Applications. 2012; 6(3):11-18. Available at: http://s3.amazonaws.com/academia.edu.documents/32964814/onl_ine_sns.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1492687149&Signature=B%2FAeIWq4LJCG61nlkV3Ihi9Beis%3D&response-content-disposition=inline%3B%20filename%3DOnline_Social_Media_Networking_and_Asses.pdf

3. Krombholz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks. Journal of Information Security and Applications. 2014; 22:1-10. Available at: http://www.sciencedirect.com/science/article/pii/S2214212614001343

4. Fire M., Goldschmidt R., Elovici Y. Online social networks: threats and solutions. Journal of Latex Class Files. 2012; 16(4):1-19. Available at: http://ieeexplore.ieee.org/abstract/document/6809839/?reload=true

5. Coppock V. Can you spot a terrorist in your classroom? Problematising the recruitment of schools to the "War on Terror" in the United Kingdom. Global Studies of Childhood. 2014; 4(2):115-125. DOI: http://dx.doi.org/10.2304/gsch.2014.4.2.115

6. Ennaji M. Recruitment of foreign male and female fighters to Jihad: Morocco's multifaceted counter-terror strategy. International Review of Sociology. 2016; 26(3):546-557. DOI: http://dx.doi.org/10.1080/03906701.2016.1244954

7. Klein G. R. Ideology isn't everything: transnational terrorism, recruitment incentives, and attack casualties. Terrorism and Political Violence. 2016; 26(5):868-887. DOI: http://dx.doi.org/10.1080/09546553.2014.961635

8. Mahood S., Rane H. Islamist narratives in ISIS recruitment propaganda. The Journal of International Communication. 2017; 23(1):1-21. DOI: http://dx.doi.org/10.1080/13216597.2016.1263231

9. Rodriguez A. B., Garcia J. S. Social networks in 20 minutos, the one survivor of free distribution press in Spain. Media and Metamedia Management. 2017. P. 429-434. DOI: http://dx.doi.org/10.1007/978-3-319-46068-0_56

10. Akbari A., Mousavi S. M. A. Criminological analysis of fraud in cyberspace. International Journal of Humanities and Cultural Studies. 2016. Special issue. April: 56-64. Available at: https://www.ijhcs.com/index.php/ijhcs/article/view/543

11. Fedushko S., Bardyn N. Algorithm of the cyber criminals identification. Global Journal of Engineering, Design & Technology. 2013; 4(2):56-62. Available at: https://www.researchgate.net/profile/Solomia_Fedushko/publication/287646809_Algorithm_of_the_cyber_criminals_identification/links/56787f5e08ae502c99d5727e.pdf

12. Nash R., Bouchard M., Malm A. Investing in people: the role of social networks in the diffusion of a large-scale fraud. Social Networks. 2013; 35(4):686-698. Available at: http://www.sciencedirect.com/science/article/pii/S0378873313000567

13. Sabillon R., Cano J., Cavaller V., Serra J. Cybercrime and cybercriminals: a comprehensive study. International Journal of Computer Networks and Communications Security. 2016; 6(4):165-176. Available at: http://www.ijcncs.org/published/volume4/issue6/p1_4-6.pdf

14. Yosefi Z., Ahmadi A. Investigating computer fraud in criminal justice system of Iran. Cumhuriyet Science Journal. 2015; 36(3):3556-3565. Available at: http://dergi.cumhuriyet.edu.tr/cumuscij/article/view/5000130788

15. Button M., McNaughton C., Kerr J. N., Owen R. Online frauds: learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology. 2014; 47(3):391-408. DOI: http://dx.doi.org/10.1177/0004865814521224

16. Savagea D., Zhanga X., Yua X., Choua P., Wanga Q. Anomaly detection in online social networks. Social Networks. 2014; 39:62-70. Available at: http://www.sciencedirect.com/science/article/pii/S0378873314000331

17. Terlutter R., Capella M. L. The gamification of advertising: analysis and research directions of in-game advertising, advergames, and advertising in social network games. Journal of Advertising. 2013; 42(2-3):95-112. DOI: http://dx.doi.org/10.1080/00913367.2013.774610

18. Waiguny M. K. J., Nelson M. R., Terlutter R. Entertainment matters! The relationship between challenge and persuasiveness of an advergame for children. Journal of Marketing Communications. 2012; 18:69-89.

19. Li S., Peitz M., Zhao X. Information disclosure and consumer awareness // Journal of Economic Behavior & Organization. 2016; 128:209-230. Available at: http://www.sciencedirect.com/science/article/pii/S0167268116300804

20. Johnson J. P. Targeted advertising and advertising avoidance. Journal of Economics. 2013; 44(1):128-144. DOI: http://dx.doi.org/10.1111/1756-2171.12014/full

21. Wang L., Wang M., Guo X., Qin X. Microblog sentiment orientation detection using user interactive relationship. Journal of Electrical and Computer Engineering. 2016; 167-181. DOI: http://dx.doi.org/10.1155/2016/7282913

22. Wang B., Zhang J., Guo H., Zhang Y., Qiao X. Model study of information dissemination in microblog community networks. Discrete Dynamics in Nature and Society. 2016; 331-354. Available at: https://www.hindawi.com/journals/ddns/2016/8393016/abs

23. Pellissier R., Nenzhelele T. E. Towards a universal competitive intelligence process model: original research. South African Journal of Information Management. 2013; 15(2):1-7. Available at: http://www.sajim.co.za/index.php/SAJIM/article/view/567

24. He W., Tian X., Chen Y., Chong D. Actionable social media competitive analytics for understanding customer experiences. Journal of Computer Information Systems. 2016; 56(2):145-155. DOI: http://dx.doi.org/10.1080/08874417.2016.1117377

25. Luu T. T. Competitive intelligence and other levers of brand performance. Journal of Strategic Marketing. 2013; 21(3):217-239. DOI: http://dx.doi.org/10.1080/0965254X.2013.765501

26. Luu T. T. Organizational social capital as a moderator for the effect of entrepreneurial orientation on competitive intelligence. Journal of Strategic Marketing. 2015; 25(4):1-15. DOI: http://dx.doi.org/10.1080/0965254X.2015.1076884

27. Tucker C. E. Social networks, personalized advertising, and privacy controls. Journal of Marketing Research. 2014; 51(5):546-562. DOI: http://dx.doi.org/10.1509/jmr.10.0355

28. Najaflou Y., Jedari B., Xia F. Safety Challenges and Solutions in Mobile Social Networks // IEEE Systems Journal. 2015; 9(3):834-854. Available at: http://ieeexplore.ieee.org/abstract/document/6642041

29. Fire M., Goldschmidt R., Elovici Y. Online social networks: threats and solutions. IEEE Communications Surveys & Tutorials. 2014; 16(4):2019-2036. Available at: http://ieeexplore.ieee.org/abstract/document/6809839

30. Young A. L., Quan-Haase A. Privacy protection strategies on Facebook. Information, Communication & Society. 2013; 16(4):479-500. DOI: http://dx.doi.org/10.1080/1369118X.2013.777757

31. Heatherly R., Kantarcioglu M., Thuraisingham B. Preventing private information inference attacks on social networks. IEEE Transactions on Knowledge and Data Engineering. 2013; 25(8):1849-1862. Available at: https://pdfs.semanticscholar.org/829c/bf93318b1e2917740b8d368f85fb922ba97f.pdf

32. Tultaeva I. V., Kaptyukhin R. V., Tultaev T. A. [The impact of social networks on communication processes in modern society]. *Vestnik Volgogradskogo instituta biznesa* = Volgograd Institute of Business Bulletin. 2014. № 4. S. 84-88. Available at: http://vestnik.volbi.ru/upload/numbers/429/article-429-970.pdf (In Russ.)

33. 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; 10(7):81-86. Available at: http://elibrary.ru/item.asp?id=26528114 (In Russ.)

34. Fedorov P. [VKontakte ahead of Instagram by the number of registered users]. Available at: http://siliconrus.com/2014/01/vkontakte-operezhaet-instagram-po-chislu-zaregistrirovannyih-polzovateley (In Russ.)

35. [Eset: Accounts of social networks of 60 % of users of RuNet were hacked by hackers]. Available at: http://www.securitylab.ru/news/442581.php (In Russ.)

36. Bartula A., Koushen A., Roberts J. J., Bouen K. N. [An empirical test social information processing theory and emotions in violent situations]. *Aktualnyye problemy ekonomiki i prava* = Actual Problems of Economics and Law. 2017; 1:189-207. Available at: http://cyberleninka.ru/article/n/empiricheskaya-proverka-teorii-obrabotki-sotsialnoy-informatsii-i-vliyanie-emotsiy-v-situatsiyah-nasiliya (In Russ.)

Submitted 15.03.2017; revised 24.04.2017; published online 14.06.2017

About the author:

Marina V. Tumbinskaya, Associate Professor of Information Security Systems Chair, Institute of Computer Technologies and Information Protection, Tupolev Kazan National Research Technical University (10 Karl Marks St., Kazan 420111, Russia), Ph.D. (Engeneering), **ORCID: http://orcid.org/0000-0003-3738-5242**, tumbinskaya@inbox.ru

The author have read and approved the final version of the manuscript.