Process of distribution of undesirable information in social networks

Marina V. Tumbinskaya
Associate Professor, Department of Information Protection Systems
Kazan National Research Technical University named after A.N. Tupolev
Address: 10, Karl Marx Street, Kazan, 420111, Russian Federation
E-mail: tumbinskaya@inbox.ru

Abstract

Currently, users of online social networks increasingly use them to promote business, distribute advertisements for goods and services, engage in leisure, hobbies, personal communication and information exchange. Thus, social networks have become an open source of information for malicious users. Hackers use various ways to implement attacks, one of which is the spread of unsolicited (targeted) information. Successful distribution of unsolicited information entails the implementation of an attack scenario and achievement of the hacker's aim. In this regard, hackers have an interest in involving so-called social networking community leaders (users who have a high level of trust and influence among a large number of community users), who are able to successfully implement part of the attack scenario of the attacker.

This article presents the results of the study in three situations: the user/potential hacker's dissemination of targeted information on the social network, receipt of targeted information by users of the social network, and counteraction and prevention of the dissemination of targeted information on the social network. Experimental data are described and their analysis is presented.

A method of protection from targeted information disseminated on social networks is identified, allowing for an increase in the level of protection of social network users' personal data and personal information and ensuring the reliability of information.

The results of the research will help prevent threats to information security, counteract attacks by hackers, who often use methods of competitive intelligence and social engineering through the use of countermeasures, develop a model of protection against targeted information and implement specialized software for its integration into social networks.

Key words: online social network, targeted information, unsolicited information, hacker, information security.

Citation: Tumbinskaya M.V. (2017) Process of distribution of undesirable information in social networks. *Business Informatics*, no. 3 (41), pp. 65–76. DOI: 10.17323/1998-0663.2017.3.65.76.

Introduction

Nowadays, everyone is an Internet user, and online social networks (OSNs) are actively developing. In literature, "microblogging" is used as a synonym for "social networks". Social networks are characterized by the ease of carrying out business promotion, the dissemination of advertisements for goods and services, leisure activities, hobbies, personal interaction and information exchange, thus serving as an open source of information for hackers. As a rule, in order to achieve their aims on social networks, hackers employ fraudulent tactics, which is confirmed by studies [1, 2]. Study [3] considers different forms of fraud on major social networks (Facebook, WhatsApp, Twitter, etc.), as well as methods and ways of combating them. One way hackers access confidential information is through the dissemination of targeted information on social networks based on methods of user manipulation [4, 5], and methods of social engineering. The concept of targeted information was formed from the concept of "targeted advertising". There is no precise definition of the concept of "targeted information". For this reason, the author of this article considers targeted information to be unsolicited information sent to a certain user or target audience in order to achieve the aim of the sender (for example, sales of goods and services, or, in the context of information security: receipt of confidential information, for example, personal data, usernames, passwords, etc.) using social resources. Research dedicated to targeted advertising on social networks are presented in study [6]. Issues of information dissemination in microblogging systems are addressed in study [7], while the effective dissemination of information on social networks are covered in study [8]. At the same time, the effectiveness of information dissemination is understood to be the level of correspondence between the results of information dissemination and the goal of information dissemination.

For their purposes, hackers may use social networking leaders for recruitment or involvement in terrorist groups [9, 10]. Often, leaders have a high level of trust among a large group of social network or community users, or are the founders (administrators) of communities [11, 12].

The scientific novelty of the study lies in the receipt of experimental data, which help to uncover the parameters of a potential hacker on social networks, underpinning methods of protection from targeted information, as well as forming recommendations for social network users to prevent information security incidents.

1. Examples of hacker implementation of cyberattacks using methods of social engineering

Let us consider examples of hacker implementation of cyberattacks using methods of social engineering. *Figure 1* presents the malicious software introduction process to the office computer of a social network user, while *Figure 2* displays a diagram of the process of corporate network server infection through malicious software. *Figure 3* is a UML diagram of the process hackers employ to use personal data in order to transfer funds.

2. Social information processing and the influence of factors on situations of dissemination of targeted information on social networks

A sample of this study features 2499 users of the Twitter, Facebook and VKontakte social networks who are moderators (administrators) of Russian user communities (the majority aged 17–30). All users participated in a test survey on situations of dissemination of unsolicited information on social networks and resistance to the dissemination of targeted information. Social network users participate in numerous situations linked to the dissemination of unsolicited information, both as victims and as potential hackers. For this reason, it is possible to study their decision-making process and factors in high-risk sit-

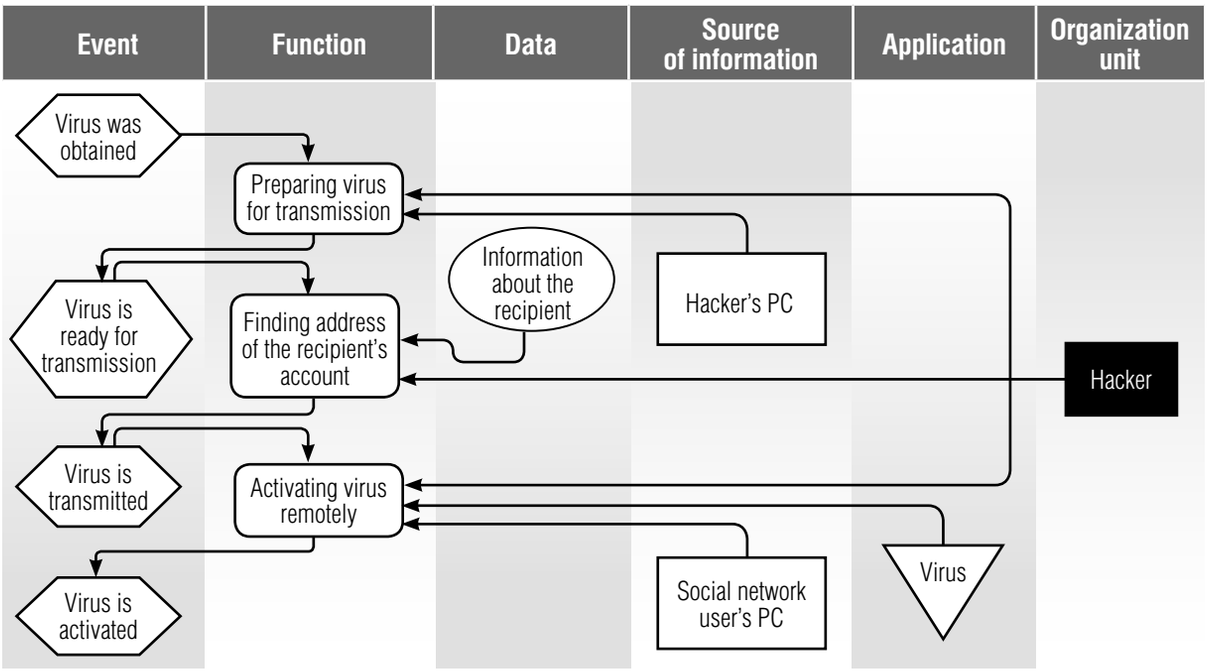

Fig. 1. Diagram of the malicious software introduction process to the office computer of a social network user

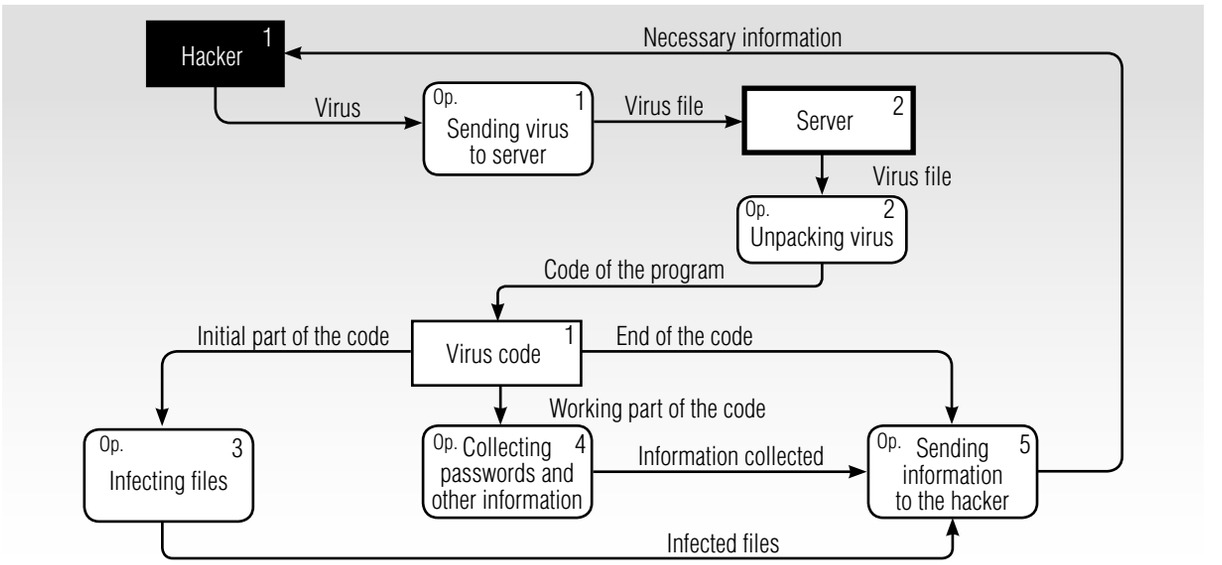

Fig. 2. DFD diagram of the process of corporate network server infection through malicious software

uations of unsolicited information dissemination on social networks.

In the study, all test surveys were anonymous and held over a six-month period in 2016–2017. A single user test survey lasted approximately one hour. The survey was held using test forms, and the results of the survey were processed using the Statistica 10.0 statistical software package. All respondents gave written consent and voluntarily agreed to participation in the survey.

The research included studies of the influence of social information processing, along with situational and personal parameters, on increased likelihood of unsolicited information dissemi-

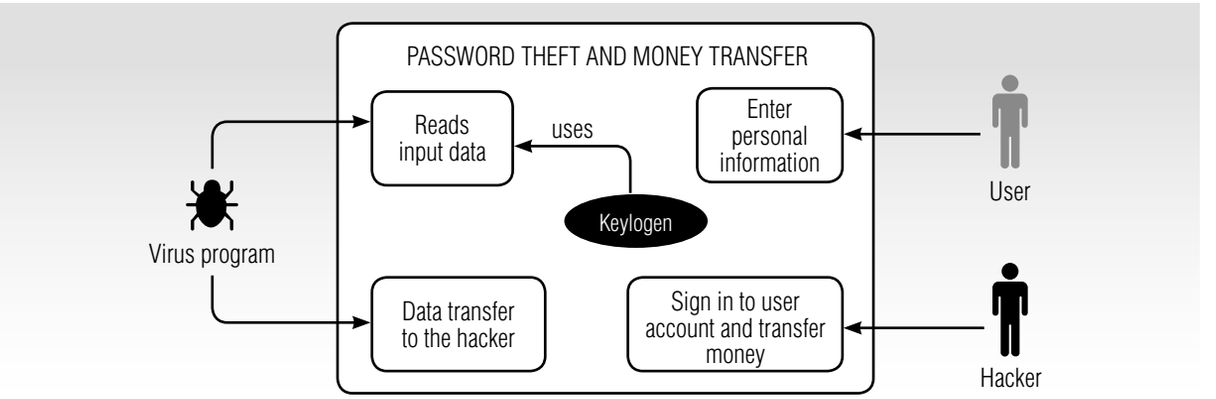

Fig. 3. UML diagram of the process hackers employ to use personal data to transfer funds

nation. To accomplish this, information was collected from respondents about the situations involving receipt and dissemination of unsolicited information that they participated in, as well as about management of those situations.

The situation of receiving targeted information is defined as potential hackers' compulsory transmission of a data message through social networks and microblogging systems to the user (potential victim) to achieve their aim. The situation of dissemination of unsolicited information involves the mass transfer by potential hackers of data messages to social network users to achieve their aim. The resistance to unsolicited information dissemination is a situation in which information dissemination, perceived by the user as possible, did not occur for any reason, for example, as a result of the blocking of a suspicious account sending spam.

The values of the test survey parameters are presented on a binary scale. All parameters take the values "0" or "1", which assists in exposing the links between them. In accordance with the social information processing theory (SIP), we are analyzing the decision-making process of hackers in situations of targeted information dissemination. SIP is a social cognitive approach based on the assumption that humans "enter social situations with a set of biologically limited possibilities and with a database of their past experience". *Table 1* shows the statistical data of a sample from 2499 respondents (with the words of the respondents).

The average age of respondents was 22 years. Nearly 75% of respondents were male. Over half of all respondents possess higher education degrees (66%). The majority of respondents indicated belonging to the lower class (70.1%), as many of them are students whose source of financial support are stipends and temporary work. The remaining respondents consider themselves part of the middle class. In 26% of cases, these are master's and graduate students who have the opportunity to work fully and pursue an academic career. Respondents' marital status statistics likewise demonstrate that during graduate level studies, students are unmarried (69%) or have a civil partner (24%), while only 7% are married.

During research, respondents reported of over 20,000 unsolicited messages received from different social network users. During the period of time under analysis, 33.4% of users received 4 — 10 messages containing unsolicited information, and only 11.7% of respondents noted that they had not received any such messages. In nearly 40% of cases, the sender of messages containing unsolicited information were unknown users, and in 30% of cases, messages were sent from fake accounts. Such messages came least often from friends (5%) and administrators (moderators) of different social network communities (5%). This statistic is due to the fact that friends rarely subject one other to that kind of dissemination, while community administrators (moderators) value their reputation.

Table 1.

Descriptive statistics of a sample of social network users

Label	Variable	Frequency	%
Gender			
n_1	Male	1874	74.99
n_2	Female	625	25.01
Age			
n_3	17–20 y.o.	450	18.01
n_4	20–24 y.o.	950	38.02
n_5	24–27 y.o.	774	30.97
n_6	27–30 y.o.	200	8.00
n_7	over 30 y.o.	125	5.00
Education			
n_8	Secondary	575	23.01
n_9	Basic vocational	275	11.00
n_{10}	Higher, baccalaureate	1049	41.98
n_{11}	Higher, specialist	200	8.00
n_{12}	Master's degree	200	8.00
n_{13}	Graduate (post-master's) degree	200	8.00
Marital status			
n_{14}	Unmarried	1725	69.03
n_{15}	I have a civil partner	599	23.97
n_{16}	Married	175	7.00
Financial situation			
n_{17}	Lower class	1774	70.99
n_{18}	Middle class	650	26.01
n_{19}	Upper class	75.	3.00
Level of knowledge in IT field			
n_{20}	Low	100	4.00
n_{21}	Medium	2025	81.03
n_{22}	High	374	14.97

Label	Variable	Frequency	%
Social network membership			
n_{23}	Twitter	525	21.00
n_{24}	Facebook	550	22.00
n_{25}	VKontakte	1424	57.00
Membership of social network community groups			
n_{26}	Hobbies, leisure	548	15.81
n_{27}	Education	575	16.58
n_{28}	Religion	577	16.65
n_{29}	Dating	630	18.17
n_{30}	Problem, disaster	552	15.92
n_{31}	Business	585	16.87
Number of followers on social network			
n_{32}	<50	999	39.98
n_{33}	50–100	625	25.01
n_{34}	100–200	375	15.01
n_{35}	200–500	375	15.01
n_{36}	>500	125	5.00
Number of friends on social network			
n_{37}	<50	125	5.00
n_{38}	50–100	500	20.01
n_{39}	100–200	1000	40.02
n_{40}	200–500	500	20.01
n_{41}	>500	374	14.97

On the content of unsolicited messages, respondents note that all proposed response options of the test survey occur: nearly 18% of instances were links to phishing sites. Values for the remaining instances ranged from 15.5% to 16.8%. These were malicious software, recruitment into terrorist groups, engagement in suspicious communities, spam, and even advertising for goods and services. 85.8% of respondents noted that there was not one cyberattack on their social network accounts, which is most likely due to the limited time period of the study (6 months). 79.8% of respondents believe contacting technical support services to be pointless.

Social network users very often ask one another for assistance in disseminating information, such as a call for help, etc. According to the statistics, the majority of respondents received such messages fewer than five times (39.2%) or did not receive any at all (13.5%). In agreeing to disseminate such messages, many respondents have more than one aim, such as financial gain (33.5%) or do it with a view to self-affirmation (25.7%). 72.6% of respondents noted that they achieved their aims through the dissemination of unsolicited information.

The dissemination of targeted information can be prevented through filtration of the data messages of social network users. 60% of respondents noted, that the number of key phrases (words) on the message filtration database ranges from 5 to 10. In addition, it is important to consider the semantics of key phrases (words) for message filtration.

The results of the study show that potential hackers can use different methods of unsolicited information dissemination depending on their aims. The simplest and fastest way to disseminate unsolicited information is the coercion or engagement of administrators (moderators) of social network communities, as they most often possess high levels of trust among users. In such cases, hackers' have high chances of achieving their aims.

Descriptive statistics (over 6 months) of a sample from 2499 users about possible situations of targeted information dissemination on social networks are shown in *Table 2*.

As a result of experimental research, three situations were considered:

1. Situations of dissemination of targeted information on social networks by users/potential hackers;

2. Situations of receipt of targeted information by social network users;

3. Situations of counteracting and preventing the dissemination of targeted information on social networks.

During studies of situation No. 1 (dissemination of targeted information on social networks by users/potential hackers), the following parameter correlation was identified.

Table 2.

Descriptive statistics of possible situations of targeted information dissemination on social networks

Values	Variable	Frequency	%
Number of recipients of unsolicited messages			
n_{41}	did not receive	293	11.72
n_{41}	under 3 times	732	29.29
n_{41}	4–10 times	835	33.41
n_{41}	11–15 times	328	13.13
n_{41}	16–20 times	210	8.40
n_{41}	over 20 times	101	4.04
Who was a sender of unsolicited messages on social networks			
n_{48}	Social network community users	500	20.01
n_{49}	Social network moderator (administrator)	125	5.00
n_{50}	Fake account	750	30.01
n_{51}	Friend	125	5.00
n_{52}	Unknown user	999	39.98
Content of unsolicited messages			
n_{53}	Link to a malicious code	388	15.53
n_{54}	Link to a phishing site	449	17.96
n_{55}	Engagement in terrorist groups	407	16.29
n_{56}	Engagement in suspicious groups	415	16.6
n_{57}	Spam	422	16.89
n_{58}	Advertisement of goods, services	418	16.73
Number of successfully-implemented cyberattacks on your account			
n_{59}	none	2145	85.83
n_{60}	under 3 times	353	14.13
n_{61}	4–10 times	1	0.04
n_{62}	11–15 times	0	0.00
n_{63}	over 15 times	0	0.00

Values	Variable	Frequency	%
Number of requests to technical support services			
n_{64}	did not contact	1994	79.79
n_{65}	under 5 times	266	10.64
n_{66}	5–20 times	204	8.16
n_{67}	20–30 times	35	1.40
n_{68}	30–50 times	0	0.00
n_{69}	over 50 times	0	0.00
Number of requests to block certain users made to social network moderators (administrators)			
n_{70}	did not contact	1637	65.51
n_{71}	under 5 times	676	27.05
n_{72}	5–20 times	142	5.68
n_{73}	20–30 times	0	0.00
n_{74}	30–50 times	44	1.76
n_{75}	over 50 times	0	0.00
Number of proposals to disseminateunsolicited information to users from your community you received as social network community moderator (administrator)			
n_{76}	none were received	337	13.49
n_{77}	under 5 times	980	39.22
n_{78}	5–20 times	690	27.61
n_{79}	20–30 times	152	6.08
n_{80}	30–50 times	171	6.84
n_{81}	over 50 times	169	6.76
What was your aim in agreeing to disseminate unsolicited data messages to your community users			
n_{82}	Financial gain	1791	33.48
n_{83}	Self-affirmation	1374	25.69
n_{84}	Revenge against social network community	77	1.44
n_{85}	Revenge against employer	207	3.87
n_{86}	Competitive intelligence	174	3.25
n_{87}	Extremism	88	1.65
n_{88}	Hooliganism	143	2.67
n_{89}	Recruitment into terrorist groups	39	0.73
n_{90}	Engagement in hacker groups	205	3.83
n_{91}	Research, interest	1251	23.39
Did you achieve your aim through dissemination of unsolicited information, having agreed to distribute data messages			
n_{92}	yes	1814	72.59
n_{93}	none	685	27.41
How many times did you contact technical support services to request blocking user accounts that disseminated unsolicited information			
n_{94}	did not contact	250	10.00
n_{95}	under 5 times	874	34.97
n_{96}	5–20 times	1000	40.02
n_{97}	20–30 times	250	10.00
n_{98}	over 30 times	125	5.00
How many key phrases / words are there in the community database (where you are moderator) for message filtration			
n_{99}	under 5	75.	3.00
n_{100}	5–10	1500	60.03
n_{101}	10–15	249	9.96
n_{102}	15–20	500	20.01
n_{103}	over 20	175	7.00
Number of users in your community			
n_{104}	≥ 50	204	8.16
n_{105}	50–150	587	23.49
n_{106}	150–300	969	38.77
n_{107}	300–500	153	6.12
n_{108}	500–1000	382	15.30
n_{109}	over 1000	204	8.16

In over 34% of instances, users of each social network (Twitter, Facebook, VKontakte) received unsolicited messages 4–10 times during the period under analysis. In 48% of cases, senders were Twitter social network community users, in 40% of cases they were fake Face-

book social network accounts, while in 34% of cases they were fake accounts on the VKontakte social network. The dissemination of unsolicited information most frequently takes place on the Twitter social network (44%). The analysis suggests that users of Twitter social network communities are inclined to disseminate targeted information. It may be assumed that the typical sender of unsolicited information on social networks is male ($n_1 \geq 60\%$), aged 20–27 years ($n_4 \geq 40\%$, $n_5 \geq 30\%$), has an undergraduate degree ($n_{10} \geq 35\%$), unmarried ($n_{14} \geq 65\%$), with a medium level of knowledge in the IT field ($n_{21} \geq 80\%$), and using the Twitter social network.

In 50% of cases, users of "problem, disaster" social network communities received data messages under three times, while in 41% of cases users of "dating" communities received messages 4–10 times. In the "education" community group, users receive unsolicited data messages from unknown users or fake accounts, which indicates hackers' choices of such a group of communities for the dissemination of information. In more than 50% of cases, dissemination is carried out by either "problem, disaster" community users (55%), thereby seeking vulnerable users for engagement in suspicious or terrorist groups, or fake accounts (50%) in "business" communities. The analysis suggests that the typical sender of unsolicited information is male ($x_1 \geq 61\%$), aged 20–27 years, has an undergraduate degree ($x_{10} \geq 33\%$), is unmarried ($x_{14} \geq 65\%$), with a medium level of knowledge in the IT field ($x_{21} \geq 50\%$), and a member of "problem, disaster", "dating", or "business" community groups.

In 31–60% of cases, social network users received unsolicited messages 4-10 times during the period under analysis (n_{44}), and, in 32–46% of cases, under 3 times. Most often (50%) senders are unknown users with over 1000 friends on social networks, in 46% of cases these are fake accounts with 200–500 friends on social networks, and in 40% under 50 friends. The analysis suggests that users with less than 50 friends on a social network are inclined to the dissemination of unsolicited information. It may be assumed that the typical sender of unsolicited information on social networks is male ($n_1 \geq 62\%$), aged 20-27 years ($n_4 \geq 36\%$, $n_5 = 62\%$), with a basic vocational ($n_9 = 40\%$) or undergraduate degree ($n_{10} \geq 41\%$), unmarried ($n_{14} \geq 50\%$), primarily with a medium level of knowledge in the IT field ($n_{21} \geq 40\%$), and possessing under 50 friends on social networks.

During studies of situation No. 2 (receipt of targeted information by social network users), the following parameter correlation was identified.

Most frequently (44%), Twitter social network users receive unsolicited messages from community users (48%) with the message information content: 2% – engagement in suspicious groups, 26% spam, 26% advertisement of goods, services. In 35% of cases, unsolicited messages are received by Facebook social network users from fake accounts (40%) with the message information content: 35% spam, 35% advertisement of goods, services. In 34% of cases, unsolicited messages are received by VKontakte social network users from fake accounts with offers advertising goods, services (31%). It may be assumed that fake accounts on Facebook and VKontakte social networks send spam and advertisements, while Twitter social network users additionally send information on engagement in suspicious groups.

In the "hobbies, leisure" and "dating" community groups of Twitter and VKontakte social networks, no more than 15% of cases of attempts to implement cyberattacks were recorded under three times. In the "hobbies, leisure" community group of the Facebook social network, hackers attempted to implement cyberattacks more than 15 times in 10% of cases. It may be assumed that potential perpetrators for the implementation of cyberattacks most frequently choose users belonging to the "hobbies, leisure" community group of Facebook social network, "problem, disaster" of Twitter social network, and "dating"

and "business" of VKontakte social network.

During studies of situation No. 3 (counteracting and preventing the dissemination of targeted information on social networks), the following parameter correlation was identified.

Users of the social networks under analysis do not contact moderators (administrators) to request blocking certain community users (≥ 52%), however, in 41% of cases, Twitter social network users contacted moderators (administrators) under 5 times. Social network users belonging to community groups n_{26}–n_{31}, most often do not contact moderators (administrators) to request blocking certain community users, or contact them rarely. This means that users do not pay sufficient attention to the informational security policies of social networks.

Most frequently (5–20 times) in 30% of cases, proposals to send messages with unsolicited content are sent to Twitter social network moderators with communities ranging from 150 to 300 users. Less often (under 5 times) in 49% of cases, proposals to send messages with unsolicited content are sent to VKontakte social network moderators with communities ranging from 150 to 300 users, and, in 45% of cases to Facebook network moderators with communities from 150 to 300 users. It may be assumed that, in order to achieve their aims, potential hackers choose to disseminate unsolicited information through moderators (administrators) of communities with 150–300 users. On the Twitter social network, the most vulnerable communities proved to be "hobbies, leisure", and "religion", on the Facebook network these were "hobbies, leisure", and on the VKontakte network "religion" and "dating".

41% of users of the social networks under analysis contact technical support services with requests to block user accounts that disseminate unsolicited information. Users of the "dating" communities of Facebook and VKontakte social networks most frequently make requests, as well as the "education" and "religion" communities of the Twitter social network.

Most often on social networks (and specifically in the "hobbies, leisure" community groups of the Facebook social network, "religion" on the Twitter social network, and "dating" on the VKontakte network) in more than 44% of cases, 5–10 key phrases are used for message filtration.

Interpretation of the research results demonstrates that potential hackers, disseminating unsolicited information containing spam and advertisements for goods and services, are: male, aged 20–27 years, with higher education, unmarried, with a medium level of knowledge in the IT field, possessing under 50 friends on social networks and concealing their data with a fake account. Most vulnerable are users belonging to "hobbies, leisure", "problem, disaster", "dating", and "business" community groups. Users rarely contact community moderators (administrators) or technical support groups in cases of the emergence of suspicious users. Most vulnerable are users/moderators (administrators) of community groups ranging from 150–300 users. The number of key phrases for the filtration of unsolicited messages (5–10) is insufficient to ensure social network information security.

3. Method for protection from the dissemination of targeted information on virtual social networks

Based on investigation of the situations of dissemination of targeted information on virtual social networks, a method for protection (*Figure 4*) is proposed, which is constituted by the steps of the following sequence:

1. Classification of social network users;
2. Protection of social network leaders;
3. Improvement of the rules of user message filtration;
4. Development of recommendations for protection from the dissemination of targeted information on social networks.

Leaders of social networks are understood to be users possessing a high level of trust and influence among a large number of community users

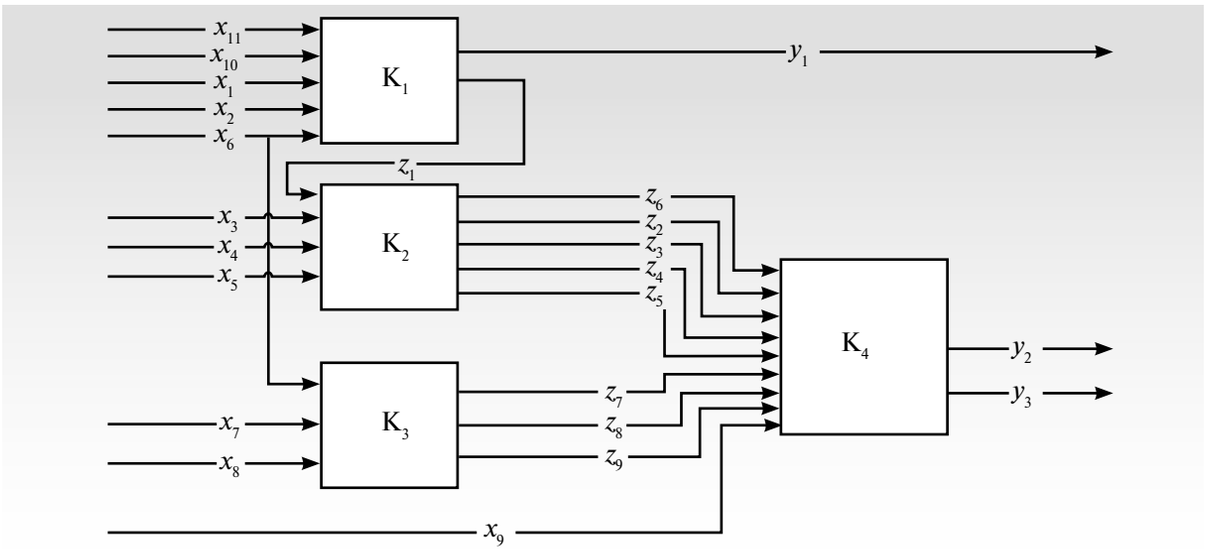

Fig. 4. Block diagram of the protection method from targeted information

capable of successfully implementing part of the actions of hackers' computer attacks. As a rule, leaders are moderators (administrators) of social network communities. This method may be formally presented in the following manner:

✦ $K = \{k_1, k_2, k_3, k_4\}$ – a set of functional blocks of the method, where k_1 – classification of social network users; k_2 – protection of social network leaders; k_3 – improvement of the rules of user message filtration; k_4 – development of recommendations for protection from the dissemination of targeted information on social networks;

✦ $X = \{x_i \mid i = \overline{1,n}\}$ – a set of input parameters, where x_1 – hacker types; x_2 – criteria of potential hacker classification; x_3 – antivirus software; x_4 – social network user/leader parameters; x_5 – parameters characterizing social network user/leader behavior; x_6 – a set of user messages; x_7 – criteria of user message information evaluation; x_8 – classification rules of user data messages; x_9 – rules of recommendation development for protection from targeted information; x_{10} – a set of social network users;

✦ $Z = \{z_\varphi \mid \varphi = \overline{1,s}\}$ – a set of internal parameters of the method, where z_1 – a list of social network leaders; z_2 – information messages on the necessity of compliance with security measures; z_3 – authentication using technical means of communication; z_4 – social network user/leader profile; z_5 – social network user/leader database; z_6 – decision-making on account blocking; z_7 – targeted information message database; z_8 – expected messages of social network users; z_9 – unsolicited messages of social network users;

✦ $Y = \{y_j \mid j = \overline{1,m}\}$ – a set of output parameters of the method, where y_1 – a list of blocked users; y_2 – information messages to social network users on possible attack implementation; y_3 – recommendations about the adoption of information security measures on social networks.

The "Classification of social network users" functional block (K_1) includes:

1) user classification based on hacker types and identification of suspicious users/potential hackers;

2) potential hacker classification based on criteria/activity (action) level with respect to social network users during a set period t_1 ;

3) decision-making on the blocking of users based on pp. 1 and 2 of this functional block;

4) classification of social network users based on "social network user/leader" types.

The "Social network leader protection" functional block (K_2) includes:

1) education and warning of network leaders: introduction of social network leader education measures on the fundamentals of information security (leader accounts are critical resources; access would allow hackers to disseminate targeted information to a large number of users) by sending information messages containing reminders about the necessity of complying with information security measure;

2) implementation of technical security measures: authentication using smart phones (telephones), the use of antivirus software, authentication using hardware, automatic password checks in compliance with information security recommendations;

3) analysis of leader behavior on social networks: development of user profiles (identification of user parameters and their threshold values), creation of databases of user activity, upgrade of user activity databases, classification of user behavior on social networks, development of models of dynamic changes in user profiles and an algorithm of abnormal user behavior identification. If user behavior on networks is abnormal, then a notification is sent informing the user of suspicious activity and subsequently blocking the account.

The "Improvement of the rules of user message filtration" functional block (K_3) is broken down into the following steps:

1) formation of a database of user messages containing targeted information disseminated on social networks, based on analyses of blocked user data;

2) development of criteria for the evaluation of user message information;

3) formation of a rule base of user message information classification;

4) database detailing of users messages containing targeted information, and their classification as expected or unsolicited based on evaluation criteria;

5) improvement of the classification rule base;

6) development of social network user message filtration model.

The "Development of recommendations for protection from the dissemination of targeted information on social network" functional block (K_4) is broken down into the following steps:

1) formation of a rule base of recommendation development for protection from targeted information;

2) social network user notification about the possible implementation of an attack (the likelihood of implementation);

3) development of recommendations on the adoption of measures to ensure information security.

We see prospects of further research of the issue of protection from targeted information in detailed study of the method and development of models of protection from targeted information on its basis. A model of protection from targeted information on social networks permits the implementation of specialized software for its integration in the major social networks, which will help users increase the security of personal information use on social networks and avoid falling prey to hackers. It is anticipated that the specialized software will be a program module (application) permitting:

✧ filtration of the personal messages and messages/records (posts) of social network community users based on the message filtration model;

✧ automatic blocking of users who send unsolicited information based on hacker types and rule bases on user blocking;

✧ provide recommendations to social network administrators (moderators) on possible threats of hacker attack implementation and the adoption of countermeasures to prevent cyberattacks on social networks.

Conclusion

The method of protection from targeted information on social networks proposed in the study facilitates the prevention of threats to information

security, prevention of hacker attempts to implement social engineering attacks, development of a model of protection from targeted information and, in the future, implement specialized software for its integration into virtual social network systems. This all will allow for external monitoring of events on social networks, as well as implementation of a search for vulnerabilities in the mechanisms of instant message exchange in order to lower the possibility of hacker attack implementation and to protect the personal information of social network users. The results of the study permit the development of recommendations for social network users to prevent incidents:

✦ apply and regularly update antivirus protection tools;

✦ update account passwords at least once a month;

✦ be more attentive to the information content of social network user messages, as links to malicious software may be concealed in the guise of advertising links;

✦ be selective in opening messages in the "hobbies, leisure", "problem, disaster", "dating", and "business" community groups;

✦ comply with social network security policies;

✦ contact community moderators (administrators) in cases of emergence of suspicious users;

✦ contact technical support groups in cases of emergence of suspicious users;

✦ in cases of moderation (administration) of community groups ranging from 150–300 users, check the content of messages sent to users;

✦ increase the number of key phrases for unsolicited message filtration.

The results of the study allow for the application of an actively evolving network approach to the study of informal communities on a new level, thereby receiving interesting and illustrative results. ■

References

1. Bradbury D. (2012) Spreading fear on Facebook. *Network Security,* no. 10, pp. 15–17.
2. Kim H.J. (2012) Online social media networking and assessing its security risks. I*nternational Journal of Security and Its Applications*, vol. 6, no. 3, pp. 11–18.
3. Savage D., Zhang X., Yu X., Chou P., Wang Q. (2014) Anomaly detection in online social networks. *Social Networks*, no. 39, pp. 62–70.
4. Krombholz K., Hobel H., Huber M., Weippl E. (2015) Advanced social engineering attacks. *Journal of Information Security and Applications*, no. 22, pp. 113–122.
5. Richard G.B., William B.B., Lewis C. (2012) Flying under the radar: Social engineering. *International Journal of Accounting and Information Management*, vol. 20, no. 4, pp. 335–347.
6. Johnson J.P. (2013) Targeted advertising and advertising avoidance. *RAND Journal of Economics*, vol. 44, no. 1, pp. 128–144.
7. Wang L., Wang M., Guo X., Qin X. (2016) Microblog sentiment orientation detection using user interactive relationship. *Journal of Electrical and Computer Engineering*, vol. 2016, pp. 167–181.
8. Khalilov D. (2013) *Marketing v sotsial'nykh setyakh* [Marketing in social networks]. Moscow: Mann, Ivanov and Ferber (in Russian).
9. *Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii* [Doctrine of information security of the Russian Federation]. Available at: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (accessed 18 May 2017) (in Russian).
10. Klein G.R. (2015) Ideology isn't everything: Transnational terrorism, recruitment incentives, and attack casualties. *Terrorism and Political Violence*, pp. 868–887. Available at: http://www.tandfonline.com/doi/full/10.1080/09546553.2014.961635 (accessed 20 January 2017).
11. Murzin F.A., Batura T.V., Proskuryakov A.V. (2015) Programmnyy kompleks dlya analiza dannykh iz sotsial'nykh setey [Software package from social networks data analysis]. *Programmnye produkty i sistemy*, no 4, pp. 188–197 (in Russian).
12. Nazarov A.N., Galushkin A.I., Sychev A.K. (2016) Risk-modeli i kriterii informatsionnogo protivoborstva v sotsial'nykh setyakh [Risk models and information confrontation criteria in social networks]. *T-Comm: Telecommunications and Transport*, vol. 10, no. 7, pp. 81–86 (in Russian).