Процесс распространения нежелательной информации в социальных сетях

М.В. Тумбинская
кандидат технических наук
доцент кафедры систем информационной безопасности
Казанский национальный исследовательский технический университет им. А.Н. Туполева
Адрес: 420111, г. Казань, ул. К. Маркса, д. 10
E-mail: tumbinskaya@inbox.ru

Аннотация

В настоящее время все чаще пользователи социальных сетей активно используют их для продвижения бизнеса, распространения рекламы товаров и услуг, досуга, хобби, личного общения и обмена информацией. Тем самым социальные сети становятся открытым источником информации для злоумышленников. Злоумышленники используют различные способы реализации атак, одним из которых является распространение нежелательной (таргетированной) информации. Успешное распространение нежелательной информации влечет реализацию сценария атаки и достижение цели злоумышленника. В связи с этим у злоумышленников появляется интерес вовлечения в процесс реализации атаки так называемых лидеров сообществ социальных сетей (пользователей, которые имеют высокий уровень доверия, влияния среди большого числа пользователей сообществ), способных успешно реализовать часть действий сценария атаки злоумышленника.

В статье представлены результаты исследования в трех ситуациях: распространение пользователем – потенциальным злоумышленником таргетированной информации в социальной сети, получение таргетированной информации пользователями социальной сети, противодействие и предотвращение распространению таргетированной информации в социальной сети. Описаны экспериментальные данные и представлена их интерпретация. Предложена методика защиты от таргетированной информации, распространяемой в социальных сетях, которая позволит повысить уровень защищенности персональных данных и личной информации пользователей социальных сетей и обеспечить достоверность информации.

Результаты исследования позволят предотвратить угрозы информационной безопасности, противодействовать атакам злоумышленников, которые зачастую используют методы конкурентной разведки и социальной инженерии за счет применения мер противодействия, разработать модель защиты от таргетированной информации и реализовать специальное программное обеспечение для его интегрирования в социальные сети.

Ключевые слова: виртуальная социальная сеть, таргетированная информация, нежелательная информация, злоумышленник, информационная безопасность.

Цитирование: Тумбинская М.В. Процесс распространения нежелательной информации в социальных сетях // Бизнес-информатика. 2017. №. 3 (41). С. 65–76.
DOI: 10.17323/1998-0663.2017.3.65.76.

Введение

В настоящее время каждый человек является пользователем интернет-пространства, активно развиваются виртуальные социальные сети (online social networks, OSNs). В литературе в качестве синонима понятия «социальные сети» также используется понятие «микроблоггинг». Социальные сети характеризуются простотой реализации продвижения бизнеса, распространения рекламы товаров и услуг, досуга, хобби, личного общения и обмена информацией, тем самым явля-

ясь открытым источником информации для злоумышленников. Как правило, для достижения своих целей в социальной сети злоумышленники применяют мошеннические схемы, что подтверждается исследованиями [1, 2]. В работе [3] рассматриваются различные способы мошенничества в наиболее распространенных социальных сетях (Facebook, WhatsApp, Twitter и т.д.), а также методы и способы борьбы с ними. В качестве одного из способов получения конфиденциальной информации злоумышленники используют распространение таргетированной информации в социальных сетях на основе методов манипуляции пользователей [4, 5] и социальной инженерии. Понятие таргетированной информации порождено понятием «таргетированная реклама». Четкого определения понятия «таргетированная информация» нет, поэтому под таргетированной информацией автор статьи понимает нежелательную информацию, навязанную конкретному пользователю или целевой группе пользователей для достижения поставленной цели отправителя (например, продажи товаров и услуг, либо, в контексте информационной безопасности, – получение конфиденциальной информации, например, персональных данных, логинов, паролей и т.д.) посредством социальных ресурсов. Исследования, посвященные таргетированной рекламе в социальных сетях, представлены в работе [6]. Вопросы распространения информации в системах микроблоггинга рассмотрены в работе [7], эффективного распространения информации в социальных сетях – в работе [8]. При этом под эффективностью распространения информации понимается степень соответствия результатов распространения информации цели распространения информации.

Для своих целей злоумышленники могут использовать лидеров социальных сетей, например, для вербовки или вовлечения в террористические группировки [9, 10]. Чаще всего лидеры имеют высокий уровень доверия среди большого числа пользователей социальных сетей или сообщества, либо являются создателями (администраторами) сообществ [11, 12].

Научная новизна работы заключается в получении экспериментальных данных, позволяющих выявить параметры потенциального злоумышленника в социальных сетях, которые заложены в основу методики защиты от таргетированной информации, а также сформировать рекомендации для пользователей социальных сетей по предотвращению инцидентов информационной безопасности.

1. Примеры реализации злоумышленниками кибератак с использованием методов социальной инженерии

Рассмотрим примеры реализации кибератак злоумышленниками, использующими методы социальной инженерии. На *рисунке 1* представлен

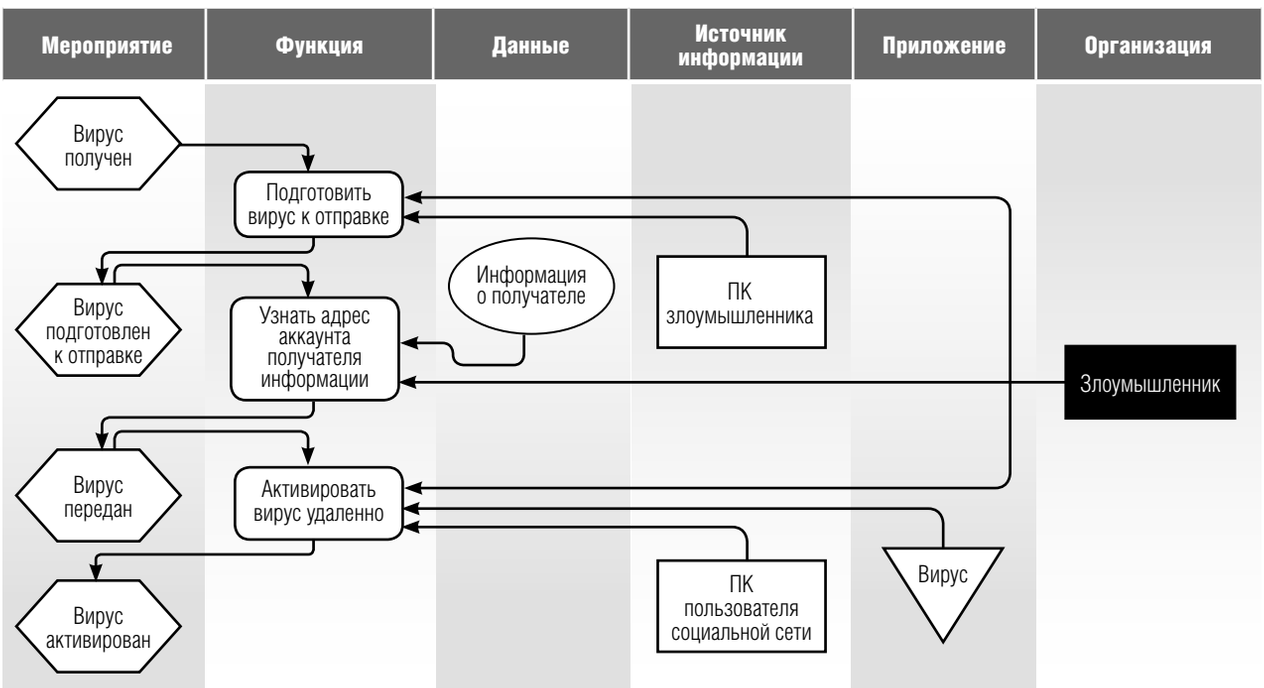

Рис. 1. Диаграмма процесса внедрения вредоносного программного обеспечения в рабочий компьютер пользователя социальной сети

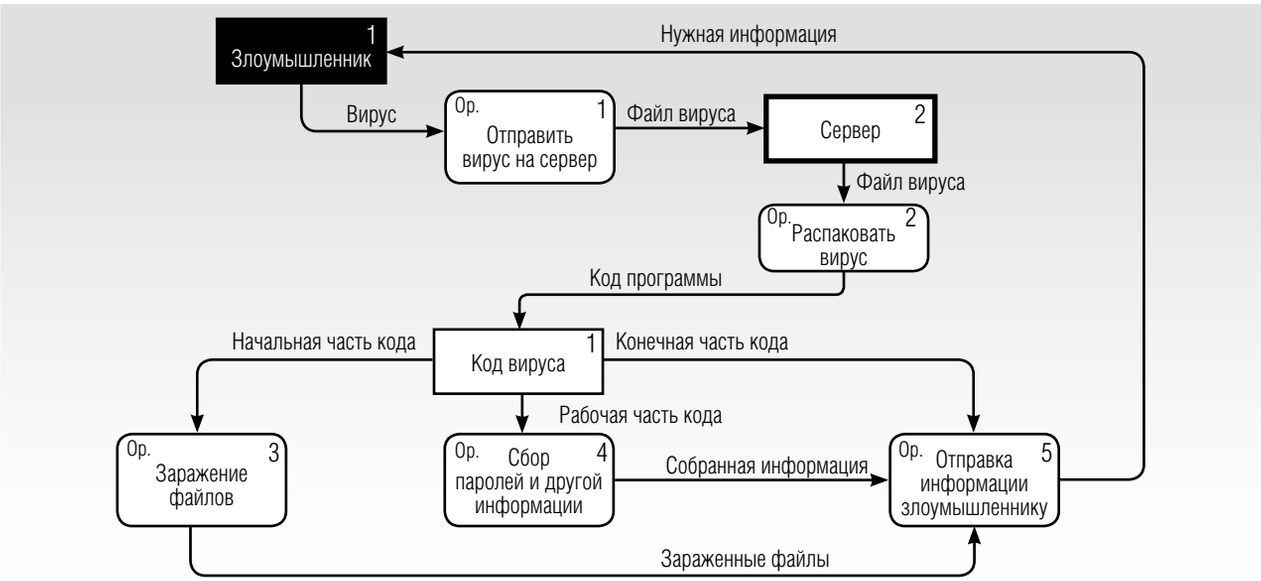

Рис. 2. DFD-диаграмма процесса заражения сервера корпоративной сети вредоносным программным обеспечением

процесс внедрения вредоносного программного обеспечения в рабочий компьютер пользователя социальной сети, на *рисунке 2* – диаграмма процесса заражения сервера корпоративной сети вредоносным программным обеспечением, а на *рисунке 3* – UML-диаграмма процесса использования злоумышленником данных пользователей для перевода денежных средств.

2. Обработка социальной информации и влияние факторов в ситуациях распространения таргетированной информации в социальных сетях

Выборка данного исследования представляет собой 2499 пользователей социальных сетей Twitter, Facebook и ВКонтакте, являющихся модераторами (администраторами) сообществ пользователей России (в большинстве – молодежь в возрасте от 17 до 30 лет). Все пользователи участвовали в тестовом опросе, касающемся ситуаций распространения нежелательной информации в социальных сетях и противодействия распространению таргетированной информации. Пользователи социальных сетей участвуют в многочисленных ситуациях, связанных с распространением нежелательной информации, как в роли жертвы, так и в роли потенциального злоумышленника. Благодаря этому на них можно изучать процесс принятия решения и факторы в ситуациях повышенного риска распространения нежелательной информации в социальных сетях.

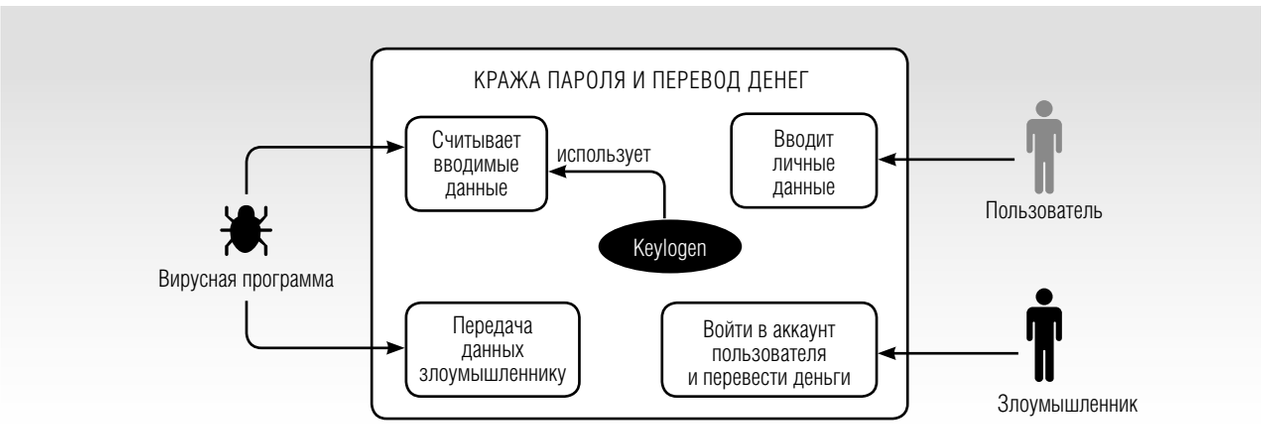

Рис. 3. UML-диаграмма процесса использования злоумышленником данных пользователей для перевода денежных средств

В исследовании все тестовые опросы являлись анонимными и проводились в течение шести месяцев 2016–2017 гг. Один тестовый опрос пользователя длился около одного часа. Опрос проводился с помощью тестовых бланков, результаты опроса обрабатывались в статистическом пакете Statistica 10.0. Все респонденты дали письменное согласие и добровольно согласились на участие в исследовании.

В ходе исследования изучалось влияние обработки социальной информации, ситуационных и личностных параметров на повышение вероятности распространения нежелательной информации. Для этого была собрана информация от респондентов о ситуациях получения и распространения нежелательной информации, в которых они участвовали, а также о купировании таких ситуаций.

Ситуация получения таргетированной информации определяется как принудительное доведение потенциальным злоумышленником информационного сообщения средствами социальных сетей и систем микроблоггинга до пользователя (потенциальной жертвы) для достижения своей цели. Ситуация распространения нежелательной информации предполагает массовую передачу потенциальным злоумышленником информационных сообщений пользователям социальных сетей 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, в результате блокировки 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». В *таблице 1* приведены статистические данные выборки из 2499 респондентов (со слов респондентов).

Таблица 1.

Описательная статистика выборки пользователей социальных сетей

Обозначение	Переменная	Частота	%
Половая принадлежность			
n_1	Мужчина	1874	74,99
n_2	Женщина	625	25,01
Возраст			
n_3	от 17 до 20 лет	450	18,01
n_4	от 20 до 24 лет	950	38,02
n_5	от 24 до 27 лет	774	30,97
n_6	от 27 до 30 лет	200	8,00
n_7	более 30 лет	125	5,00
Образование			
n_8	Среднее	575	23,01
n_9	Начальное профессиональное	275	11,00
n_{10}	Высшее бакалавриат	1049	41,98
n_{11}	Высшее специалитет	200	8,00
n_{12}	Магистратура	200	8,00
n_{13}	Аспирантура	200	8,00
Семейное положение			
n_{14}	Холост	1725	69,03
n_{15}	Имею гражданского партнера	599	23,97
n_{16}	В браке	175	7,00
Финансовое положение			
n_{17}	Низший класс	1774	70,99
n_{18}	Средний класс	650	26,01
n_{19}	Высший класс	75	3,00
Уровень знаний в сфере ИТ			
n_{20}	Низкий	100	4,00
n_{21}	Средний	2025	81,03
n_{22}	Высокий	374	14,97
Принадлежность к социальной сети			
n_{23}	Twitter	525	21,00
n_{24}	Facebook	550	22,00
n_{25}	ВКонтакте	1424	57,00
Принадлежность к группам сообществ социальной сети			
n_{26}	Хобби, развлечения	548	15,81
n_{27}	Обучение	575	16,58
n_{28}	Религия	577	16,65
n_{29}	Знакомства	630	18,17
n_{30}	Проблема, беда	552	15,92
n_{31}	Бизнес	585	16,87
Количество подписчиков в социальной сети			
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
Количество друзей в социальной сети			
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

Средний возраст респондентов составил 22 года. Из них почти 75% составляют мужчины, остальные – женщины. Более половины, респондентов имеют законченное высшее образование (66%). Большинство респондентов указали на принадлежность к низшему классу (70,1%), поскольку многие из них – студенты, основным источником которых являются стипендия и случайный заработок. Остальные респонденты относят себя к среднему классу, в 26% случаев это магистранты и аспиранты, которые имеет возможность полноценно трудиться и заниматься наукой. Статистика семейного положения респондентов также свидетельствует о том, что студенты в период получения высшего образования не состоят в браке 69%, имеют гражданского партнера 24%, а в официальном браке состоят всего 7%.

В ходе исследования респонденты сообщили более чем о 20 тысячах нежелательных сообщений, поступивших от различных пользователей социальных сетей. За анализируемый промежуток времени 33,4% пользователей получали от 4 до 10 сообщений, содержащих нежелательную информацию, и лишь 11,7% респондентов отметили, что не получали подобных сообщений. В почти 40% случаев отправителем сообщений, содержащих нежелательную информацию, являлись неизвестные пользователи, а в 30% случаев сообщения отправлялись с фейковых аккаунтов. Реже всего такие сообщения приходят от друзей (5%) и администраторов (модераторов) различных сообществ социальных сетей (5%). Данная статистика объясняется тем, что друзья редко подвергают друг друга такого рода рассылкам, а администраторы (модераторы) сообществ дорожат своей репутацией.

По содержанию нежелательных сообщений респонденты отмечают, что все предложенные варианты ответов тестового опроса имеют место: почти в 18% случаев – это ссылка на фишинговые сайты, в остальных случаях значения составляли от 15,5% до 16,8%. Это вредоносные программы, вербовка в террористические группы, вовлечение в сомнительные сообщества, спам и даже реклама товаров и услуг. 85,8% респондентов отметили, что на их аккаунты в социальных сетях не было ни одной кибератаки, что, вероятнее всего, обусловлено ограничением времени исследования (6 месяцев). 79,8% респондентов считают, что обращение в службу технической поддержки нецелесообразно.

Очень часто в социальных сетях пользователи просят друг другу помочь в рассылке какой-либо информации, например, призыв о помощи и т.п. По статистике, большинству респондентов подобного рода сообщения поступали менее пяти раз (39,2%) или вовсе не поступали (13,5%). Соглашаясь на рассылку подобного рода сообщений, многие респонденты преследуют более чем одну цель, например, финансовую выгоду (33,5%) или делают это с целью самоутверждения (25,7%). 72,6% респондентов отметили, что достигли своих целей средствами рассылки информации нежелательного содержания.

Рассылку таргетированной информации можно предотвратить путем фильтрации информационных сообщений пользователей социальных сетей. Так 60% респондентов отметили, что число ключевых словосочетаний (слов) в базе данных фильтрации сообщений составляет от 5 до 10. Кроме того, следует учитывать семантику ключевых словосочетаний (слов) для фильтрации сообщений.

Результат исследования показывает, что потенциальный злоумышленник может использовать различные способы распространения нежелательной информации, в зависимости от поставленных целей. Самым простым и краткосрочным способом распространения нежелательной информации является принуждение или привлечение администраторов (модераторов) сообществ в социальных сетях, т.к. они чаще всего обладают высоким уровнем доверия среди пользователей. В таких случаях и вероятность достижения злоумышленником своих целей высока.

Описательная статистика (за 6 месяцев) выборки из 2499 пользователей о возможных ситуациях распространения таргетированной информации в социальных сетях приведена в *таблице 2.*

В результате экспериментального исследования было рассмотрено три ситуации:

1. Ситуация распространения пользователем – потенциальным злоумышленником таргетированной информации в социальной сети;

2. Ситуация получения таргетированной информации пользователями социальной сети;

3. Ситуация противодействия и предотвращения распространению таргетированной информации в социальной сети.

В рамках исследования ситуации №1 (распространение пользователем – потенциальным злоумышленником таргетированной информации в социальной сети) была выявлена следующая взаимосвязь параметров.

Таблица 2.

Описательная статистика возможных ситуаций распространения таргетированной информации в социальных сетях

Обозначение	Переменная	Частота	%
Количество получаемых сообщений нежелательного содержания			
n_{42}	не получал	293	11,72
n_{43}	менее 3 раз	732	29,29
n_{44}	от 4 до 10 раз	835	33,41
n_{45}	от 11 до 15 раз	328	13,13
n_{46}	от 16 до 20 раз	210	8,40
n_{47}	более 20 раз	101	4,04
Кто являлся отправителем сообщений нежелательного содержания в социальной сети			
n_{48}	Пользователи сообществ социальной сети	500	20,01
n_{49}	Модератор (администратор) социальной сети	125	5,00
n_{50}	Фейковый аккаунт	750	30,01
n_{51}	Друг	125	5,00
n_{52}	Неизвестный пользователь	999	39,98
Содержание нежелательных сообщений			
n_{53}	Ссылка на вредоносный код	388	15,53
n_{54}	Ссылка на фишинговый сайт	449	17,96
n_{55}	Вовлечение в террористические группы	407	16,29
n_{56}	Вовлечение в сомнительные группы	415	16,6
n_{57}	Спам	422	16,89
n_{58}	Реклама товаров, услуг	418	16,73
Количество кибератак на Ваш аккаунт, которые были успешно реализованы			
n_{59}	нет	2145	85,83
n_{60}	менее 3 раз	353	14,13
n_{61}	от 4 до 10 раз	1	0,04
n_{62}	от 11 до 15 раз	0	0,00
n_{63}	более 15 раз	0	0,00
Количество обращений в службу технической поддержки			
n_{64}	не обращался	1994	79,79
n_{65}	менее 5 раз	266	10,64
n_{66}	от 5 до 20 раз	204	8,16
n_{67}	от 20 до 30 раз	35	1,40
n_{68}	от 30 до 50 раз	0	0,00
n_{69}	более 50 раз	0	0,00
Количество обращений к модератору (администратору) социальной сети с просьбой заблокировать определенного пользователя			
n_{70}	не обращался	1637	65,51
n_{71}	менее 5 раз	676	27,05
n_{72}	от 5 до 20 раз	142	5,68
n_{73}	от 20 до 30 раз	0	0,00
n_{74}	от 30 до 50 раз	44	1,76
n_{75}	более 50 раз	0	0,00

Обозначение	Переменная	Частота	%
Количество предложений сделать рассылку информационных сообщений нежелательного содержания пользователям вашего сообщества, поступивших вам, как модератору (администратору) сообщества социальной сети			
n_{76}	не поступали	337	13,49
n_{77}	менее 5 раз	980	39,22
n_{78}	от 5 до 20 раз	690	27,61
n_{79}	от 20 до 30 раз	152	6,08
n_{80}	от 30 до 50 раз	171	6,84
n_{81}	более 50 раз	169	6,76
Какую цель вы преследовали, соглашаясь на рассылку информационных сообщений нежелательного содержания пользователям вашего сообщества			
n_{82}	Финансовая выгода	1791	33,48
n_{83}	Самоутверждение	1374	25,69
n_{84}	Месть сообществу социальной сети	77	1,44
n_{85}	Месть работодателю	207	3,87
n_{86}	Конкурентная разведка	174	3,25
n_{87}	Экстремизм	88	1,65
n_{88}	Хулиганство	143	2,67
n_{89}	Вербовка в террористические группы	39	0,73
n_{90}	Вовлечение в группы злоумышленников	205	3,83
n_{91}	Исследование, интерес	1251	23,39
Достигли ли вы своей цели, путем распространения нежелательной информации согласившись на рассылку информационных сообщений			
n_{92}	да	1814	72,59
n_{93}	нет	685	27,41
Сколько раз вы обращались в службу технической поддержки с просьбой заблокировать аккаунт пользователя, распространяющего нежелательную информацию			
n_{94}	не обращался	250	10,00
n_{95}	менее 5 раз	874	34,97
n_{96}	от 5 до 20 раз	1000	40,02
n_{97}	от 20 до 30 раз	250	10,00
n_{98}	более 30 раз	125	5,00
Сколько ключевых словосочетаний / слов в базе данных сообщества (где вы являетесь модератором) для фильтрации сообщений			
n_{99}	менее 5	75	3,00
n_{100}	от 5 до 10	1500	60,03
n_{101}	от 10 до 15	249	9,96
n_{102}	от 15 до 20	500	20,01
n_{103}	более 20	175	7,00
Количество пользователей в вашем сообществе			
n_{104}	≤ 50	204	8,16
n_{105}	от 50 до 150	587	23,49
n_{106}	от 150 до 300	969	38,77
n_{107}	от 300 до 500	153	6,12
n_{108}	от 500 до 1000	382	15,30
n_{109}	более 1000	204	8,16

В более чем 34% случаев пользователи каждой из социальных сетей (Twitter, Facebook, ВКонтакте) получали нежелательные сообщения от 4 до 10 раз за анализируемый период. В 48% случаях отправителями являлись пользователи сообществ социальной сети Twitter, в 40% случаях – фейковый аккаунт социальной сети Facebook, а в 34% случаях – социальной сети ВКонтакте. Чаще всего распространение нежелательной информации происходит в социальной сети Twitter (44%). Анализ позволяет сделать вывод, что пользователи сообществ социальной сети Twitter склонны к распространению таргетированной информации. Можно предположить, что типовой отправитель нежелательной информации в социальной сети – мужчина ($n_1 \geq 60\%$) в возрасте от 20 до 27 лет ($n_4 \geq 40\%$, $n_5 \geq 30\%$), с высшим бакалаврским образованием ($n_{10} \geq 35\%$), холостой ($n_{14} \geq 65\%$), со средним уровнем знаний в сфере ИТ ($n_{21} \geq 80\%$), использующий социальную сеть Twitter.

В 50% случаев пользователи сообществ «проблема, беда» социальной сети получали информационные сообщения менее трех раз, в 41% случаях от 4 до 10 раз сообщения получали пользователи сообщества «знакомства». В группе сообщества «обучение» пользователи получают информационные сообщения нежелательного содержания от неизвестных пользователей, фейковых аккаунтов, что говорит о выборе злоумышленником подобного рода групп сообществ для распространения информации. Более чем в 50% случаев распространением занимаются либо пользователи сообществ «проблема, беда» (55%), тем самым выискивая уязвимых пользователей для вовлечения в сомнительные или террористические группы, либо фейковые аккаунты (50%) в сообществах «бизнес». Анализ позволяет сделать вывод, что типовой отправитель нежелательной информации – мужчина ($x_1 \geq 61\%$) в возрасте от 20 до 27 лет, с высшим образованием бакалавриата ($x_{10} \geq 33\%$), холостой ($x_{14} \geq 65\%$), со средним уровнем знаний в сфере ИТ ($x_{21} \geq 50\%$), состоящий в группах сообществ «проблема, беда», «знакомства» или «бизнес».

В 31–60% случаев пользователи социальной сети получали нежелательные сообщения от 4 до 10 раз за анализируемый период (n_{44}), в 32–46% случаев – менее трех раз. Чаще всего (50%) отправителем является неизвестный пользователь, имеющий более 1000 друзей в социальной сети, в 46% случаев – фейковый аккаунт, имеющий от 200 до 500 друзей в социальной сети, в 40% – меньше 50 друзей. Анализ позволяет сделать вывод, что пользователи, имеющие менее 50 друзей в социальной сети, склонны к распространению нежелательной информации. Можно предположить, что типовой отправитель нежелательной информации в социальной сети – мужчина ($n_1 \geq 62\%$) в возрасте от 20 до 27 лет ($n_4 \geq 36\%$, $n_5 = 62\%$), с начальным профессиональным ($n_9 = 40\%$) или с высшим образованием бакалавриата ($n_{10} \geq 41\%$), холостой ($n_{14} \geq 50\%$), преимущественно со средним уровнем знаний в сфере ИТ ($n_{21} \geq 40\%$), имеющим менее 50 друзей в социальной сети.

В рамках исследования ситуации №2 (получение таргетированной информации пользователями социальной сети) была выявлена следующая взаимосвязь параметров.

Чаще всего (44%) пользователи социальной сети Twitter получают нежелательные сообщения от пользователей сообществ (48%) с информационным контентом сообщений: 26% – вовлечение в сомнительные группы, 26% – спам, 26% – реклама товаров, услуг. В 35% случаев нежелательные сообщения получают пользователи социальной сети Facebook, от фейковых аккаунтов (40%) с информационным контентом сообщений: 35% – спам, 35% – реклама товаров, услуг. В 34% случаях нежелательные сообщения получают пользователи социальной сети ВКонтакте, от фейковых аккаунтов с предложением рекламы товаров, услуг (31%). Можно предположить, что фейковые аккаунты социальных сетей Facebook и ВКонтакте рассылают спам и рекламу, а пользователи социальной сети Twitter еще и информацию по вовлечению в сомнительные группы.

В группах сообществ «хобби, развлечения» и «знакомства» социальных сетей Twitter и ВКонтакте не более, чем в 15% случаев попытки реализации кибератак зафиксированы менее трех раз. В группе сообществ «хобби, развлечения» социальной сети Facebook злоумышленники пытались реализовать кибератаки более 15 раз в 10% случаев. Можно предположить, что чаще всего потенциальные нарушители для реализации кибератак выбирают пользователей, принадлежащих к группам сообществ «хобби, развлечения» социальной сети Facebook, «проблема, беда» – социальной сети Twitter, «знакомства» и «бизнес» – социальной сети ВКонтакте.

В рамках исследования ситуации №3 (противодействие и предотвращение распространения таргетированной информации в социальной сети) была выявлена следующая взаимосвязь параметров.

Пользователи анализируемых социальных сетей не обращаются к модераторам (администраторам) с просьбой заблокировать конкретного пользователя сообщества (≥ 52%), однако в 41% случаев пользователи социальной сети Twitter обращались с просьбой к модератору (администратору) менее 5 раз. Пользователи социальных сетей, принадлежащих к группам сообществ n_{26}–n_{31}, чаще всего не обращаются к модераторам (администраторам) с просьбой заблокировать конкретного пользователя сообщества, либо обращаются редко. Это означает, что пользователи не уделяют должного внимания политике информационной безопасности социальных сетей.

Чаще всего (от 5 до 20 раз) в 30% случаев поступают предложения сделать рассылку сообщений, содержащих нежелательную информацию модераторам социальной сети Twitter с сообществами составом от 150 до 300 пользователей. Реже (менее 5 раз) в 49% случаях поступают предложения сделать рассылку сообщений, содержащих нежелательную информацию модераторам социальной сети ВКонтакте с сообществами составом от 150 до 300 пользователей, в 45% случаях – модераторам сети Facebook с сообществами составом от 150 до 300 пользователей. Можно предположить, что потенциальный злоумышленник выбирает для достижения цели распространение нежелательной информации через модераторов (администраторов) сообществ, имеющих состав от 150 до 300 пользователей. В социальной сети Twitter наиболее уязвимыми оказались сообщества «хобби, развлечения», «религия», в сети Facebook – «хобби, развлечения», в сети ВКонтакте – «религия» и «знакомства».

41% пользователей анализируемых социальных сетей обращаются в службу технической поддержки с просьбой заблокировать аккаунт пользователя, распространяющего нежелательную информацию. Чаще всего обращаются пользователи групп сообществ «знакомства» социальных сетей Facebook и ВКонтакте, а также сообществ «обучение» и «религия» социальной сети Twitter.

Чаще всего в социальных сетях (а именно в группах сообществ «хобби, развлечение» социальной сети Facebook, «религия» социальной сети Twitter и «знакомства» сети ВКонтакте) в более чем 44% случаев для фильтрации сообщений используется от 5 до 10 ключевых словосочетаний.

Интерпретация результатов исследования демонстрирует, что потенциальный злоумышленник, распространяющий нежелательную информацию, с контентом спама, рекламы товаров, услуг, в социальных сетях – это мужчина в возрасте от 20 до 27 лет, с высшим образованием, холостой, со средним уровнем знаний в сфере ИТ, имеющий менее 50 друзей в социальной сети и скрывающий свои данные под фейковым аккаунтом. Наиболее уязвимыми являются пользователи, состоящие в группах сообществ «хобби, развлечение», «проблема, беда», «знакомства», «бизнес». Пользователи редко обращаются к модераторам (администраторам) сообществ и в группу технической поддержки в случаях возникновения подозрительных пользователей. Наиболее уязвимыми являются пользователи – модераторы (администраторы) групп сообществ с составом от 150 до 300 пользователей. Количество ключевых словосочетаний для фильтрации нежелательных сообщений (от 5 до 10) недостаточно для обеспечения информационной безопасности социальной сети.

3. Методика защиты от распространения таргетированной информации в виртуальных социальных сетях

На основе исследования ситуаций распространения таргетированной информации в виртуальных социальных сетях предлагается методика защиты (*рисунок 4*), которая представляет собой последовательность следующих шагов:

1. Классификация пользователей социальной сети;

2. Защита лидеров социальной сети;

3. Совершенствование правил фильтрации сообщений пользователей;

4. Выработка рекомендаций по защите от распространения таргетированной информации в социальной сети.

Под лидером социальной сети понимается пользователь, который имеет высокий уровень доверия и влияния среди большого числа пользователей сообществ, способных успешно реализовать часть действий сценария атаки злоумышленника, как правило являющийся модераторам (администратором) сообществ социальной сети. Формально данную методику можно представить следующим образом:

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

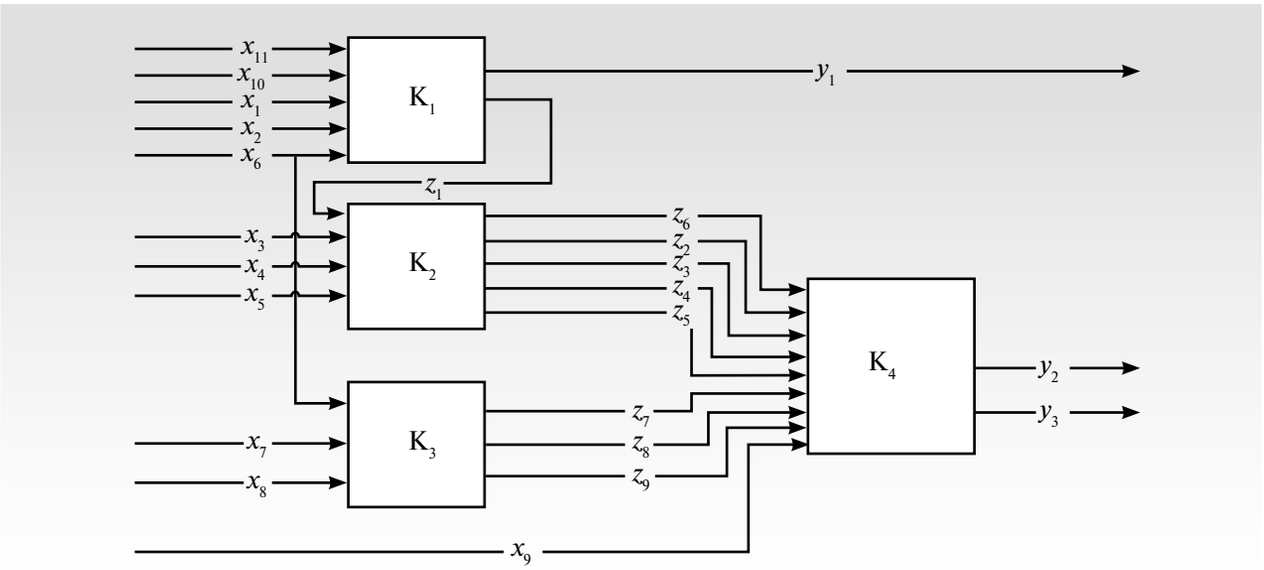

Рис. 4. Структурная схема методики защиты от таргетированной информации

нения таргетированной информации в социальной сети;

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

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

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

Функциональный блок «Классификация пользователей социальной сети» (K_1) включает:

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

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

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

4) классификацию пользователей социальной сети на основе образов «пользователь – лидер социальной сети».

Функциональный блок «Защита лидеров социальной сети» (К2) включает:

1) обучение и предостережение лидеров сети: введение мер по обучению лидеров социальной сети основам информационной безопасности (аккаунты лидеров являются критическими ресурсами, при получении доступа к которым злоумышленник сможет распространить таргетированную информацию большому числу пользователей) путем рассылки ин-

формационных сообщений, содержащих напоминания о необходимости соблюдения мер информационной безопасности;

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

3) анализ поведения лидера в социальной сети: разработка профиля пользователя (определение параметров пользователей и их граничных значений), создание базы данных действий пользователей, обновление базы данных действий пользователей, классификация поведения пользователя в социальной сети, разработка модели динамического изменения профиля пользователя и алгоритма определения аномального поведения пользователя. 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» (K_3) декомпозируется на следующие этапы:

1) формирование базы данных сообщений пользователей, содержащих таргетированную информацию, распространяемую в социальной сети 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 социальной сети.

Функциональный блок «Выработка рекомендаций по защите от таргетированной информации в социальной сети» (K_4) декомпозируется на следующие этапы:

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

2) информирование пользователя социальной сети о возможной реализации атаки (вероятность реализации);

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

Перспективы дальнейшего исследования проблемы защиты от таргетированной информации мы видим в детальной проработке методики и разработке на ее основе модели защиты от таргетированной информации. Модель защиты от таргетированной информации в социальных сетях позволит реализовать специальное программное обеспечение для его интегрирования в наиболее распространенные социальные сети, что поможет пользователям повысить безопасность использования личной информации в социальной сети и не попадаться на уловки злоумышленников. Предполагается, что специальное программное обеспечение будет представлять собой программный модуль (приложение), позволяющее:

✧ фильтровать личные сообщения пользователей, сообщений–записей (постов) пользователей сообществ социальных сетей на основе модели фильтрации сообщений;

✧ в автоматизированном режиме блокировать пользователей, рассылающих нежелательную информацию, на основе образов злоумышленников и базы правил о блокировании пользователей;

✧ предоставлять рекомендации администраторам (модераторам) социальных сетей о возможных угрозах реализации атак злоумышленниками и принятии контрмер по предотвращению кибератак в социальных сетях.

Заключение

Предложенная в работе методика защиты от таргетированной информации в социальной сети, позволит предотвратить угрозы информационной безопасности, предотвратить попытки злоумышленников реализации социоинженерных атак, разработать модель защиты от таргетированной информации и в дальнейшем реализовать специальное программное обеспечение для его интегрирования в системы виртуальной социальной сети. Все это позволит проводить внешний мониторинг событий в социальной сети, а также осуществлять поиск уязвимостей в механизмах обмена мгновенными сообщениями для снижения возможности реализации атак злоумышленниками и защиты личной информации пользователей социальных сетей. Результаты исследования позволяют сфор-

мулировать рекомендации для пользователя социальной сети по предотвращению инцидентов:

✦ применять и своевременно обновлять средства антивирусной защиты;

✦ обновлять пароль аккаунта не реже одного раза в месяц.

✦ внимательнее относиться к информационному контенту сообщений пользователей социальных сетей, поскольку под видом рекламной ссылки могут скрываться ссылки на вредоносное программное обеспечение.

✦ избирательно относиться к сообщениям в группах сообществ «хобби, развлечение», «проблема, беда», «знакомства», «бизнес»;

✦ соблюдать политику безопасности социальных сетей;

✦ обращаться к модераторам (администраторам) сообществ в случаях возникновения подозрительных пользователей;

✦ обращаться в группу технической поддержки в случаях возникновения подозрительных пользователей;

✦ в случае модерирования (администрирования) групп сообществ с составом от 150 до 300 пользователей проверять контент сообщений для рассылки пользователям;

✦ увеличить количество ключевых словосочетаний для фильтрации нежелательных сообщений.

Результаты исследования позволяют на новом уровне применять активно развивающийся сетевой подход к исследованию неформальных сообществ, получая интересные и наглядные результаты. ■

Литература

1. Bradbury D. Spreading fear on Facebook // Network Security. 2012. No. 10. P. 15–17.
2. Kim H.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.
3. Anomaly detection in online social networks / D. Savage [et al.] // Social Networks. 2014. No. 39. P. 62–70.
4. Krombholz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks // Journal of Information Security and Applications. 2015. No. 22. P. 113–122.
5. Richard G.B., William B.B., Lewis C. Flying under the radar: Social engineering // International Journal of Accounting and Information Management. 2012. Vol. 20. No. 4. P. 335–347.
6. Johnson J.P. Targeted advertising and advertising avoidance // RAND Journal of Economics. 2013. Vol. 44. No. 1. P. 128–144.
7. Wang L., Wang M., Guo X., Qin X. Microblog sentiment orientation detection using user interactive relationship // Journal of Electrical and Computer Engineering. 2016. Vol. 2016. P. 167–181.
8. Халилов Д. Маркетинг в социальных сетях. М.: Манн, Иванов и Фербер, 2013.
9. Доктрина информационной безопасности Российской Федерации. [Электронный ресурс]: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 18.05.2017).
10. Klein G.R. Ideology isn't everything: Transnational terrorism, recruitment incentives, and attack casualties // Terrorism and Political Violence. 2015. P. 868–887. Available at: http://www.tandfonline.com/doi/full/10.1080/09546553.2014.961635 (accessed 20 January 2017).
11. Мурзин Ф.А., Батура Т.В., Проскуряков А.В. Программный комплекс для анализа данных из социальных сетей // Программные продукты и системы. 2015. № 4. С. 188–197.
12. Назаров А.Н., Галушкин А.И., Сычев А.К. Риск-модели и критерии информационного противоборства в социальных сетях // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 7. С. 81–86.

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 FederatioE-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.

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).