СИСТЕМНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОТ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Тумбинская М.В.[1]

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. 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. Предложена методика защиты от таргетированной информации, распространяемой в социальных сетях на основе исследования социальной информации. Детализация сценариев атак позволит выработать меры противодействия. Методика защиты от таргетированной информации, распространяемой в социальных сетях позволит разработать модель защиты от таргетированной информации и реализовать специальное программное обеспечение для его интегрирования в социальные сети.

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

DOI: 10.21681/2311-3456-2017-2-30-44

Введение

В настоящее время почти каждый человек является пользователем интернет-пространства, активно развиваются виртуальные социальные сети – Online Социальной сети(ONS). В литературе синонимом 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 являясь открытым источником информации для злоумышленников. Злоумышленники в ONS для достижения своих целей применяют мошеннические схемы, что подтверждается исследованиями [1 – 2]. Авторы [3 – 4] рассматривают различные способы мошенничества в наиболее распространенных социальных сетях Facebook, Whatsapp, Twitter и т.д., методы и способы борьбы с ними. Злоумышленники в качестве одного из способов получения конфиденциальной информации используют распространение таргетированной информации в социальных сетях на основе методов манипуляции пользователей [5 – 6] и социальной инженерии. Понятие таргетированной информации порождено понятием «таргетированная реклама». Под таргетированной информацией понимается нежелательная информация, содержащаяся в информационных сообщениях пользователя или группы пользователей (сообщества) социальной сети. Для своих целей злоумышленники могут использовать лидеров социальной сети, например, для вербовки или вовлечения в сомнительные, либо в террористические группы. Чаще всего лидеры имеют высокий уровень доверия среди большого числа пользователей социальной сети или сообщества либо являются создателями (администраторами) сообществ [7].

Вопросы доверия лидеру и информации, обрабатываемой в системах микроблоггинга, рассмотрены в работе [8]. Одной из целей злоумышленника в распространении таргетированной информации является конкурентная разведка, обзор способов которых представлен в работе [11]. В настоящее время большое внимание исследователей уделено защите информации в социальных сетях. Так в работах [10 - 19] рассмотрены основы информационной безопасности, способы потери данных, распространенных угрозах и уязвимостях ONS.

В работе [9] рассмотрены алгоритм распространения нежелательной информации в системах ONS, который представлен в виде реализации одной из возможных диаграмм прецедентов с использованием языка UML, что недостаточно для понимания его работы, методика защиты от таргетированной информации, которая представлена тремя этапами вербального описания и не отражает процесса взаимодействия с алгоритмом.

1 Тумбинская Марина Владимировна, кандидат технических наук, Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, г. Казань, tumbinskaya@inbox.ru

В отличие от работы [9], в статье автором сделана попытка формализации обобщенного алгоритма распространения таргетированной информации в социальных сетях путем определения входных, выходных и внутренних состояний алгоритма, которые заложены в основу методики защиты от таргетированной информации. Достоинством предложенной автором статьи методики в отличие от методики, представленной в работе [9] является ее дополнение, модификация функциональных блоков и их детализация. Кроме того, автором предложена структурная схема методики защиты от распространения таргетированной информации в социальных сетях, которая отражает параметрические взаимосвязи. Отличительной особенностью работы автора Д.Х. Мирзанурова [9] является предложенный анализ методов выявления влиятельных пользователей сети в системах ONS, на основе зарубежных публикаций ученых.

Научная новизна данной статьи заключается в формализации обобщенного алгоритма распространения таргетированной информации в виртуальных социальных сетях, который заложен в основу методики защиты от таргетированной информации на основе статистического исследования.

Примеры реализации кибератак злоумышленниками методами социальной инженерии в социальных сетях

Рассмотрим примеры реализации кибератак злоумышленниками методами социальной инженерии в социальных сетях, формализация которых представлена с примененим методологии структурного анализа IDEF0. Функциональная модель (диаграмма A0, диаграмма A3) реализации кибератаки похищения денежных средств на основе метода социальной инженерии «Фишинг» представлены на рисунках 1, 2 соответственно. Данная кибератака подразумевает, что злоумышленник рассылает сообщение вредоносного содержания пользователю, на электронную почту, в системе микроблоггинга, в социальных сетях. В случае успеха (то бишь пользователь открывает сообщение вредоносного содержания) вирус заражает компьютер пользователя, крадёт данные пользователя, а также номер и пароль банковской карты, далее высылает их злоумышленнику и тот, соответственно, переводит деньги на свои счета.

На рисунках 3, 4 представлены диаграммы реализации кибератаки хищения конфиденциальных данных на основе метода социальной инженерии «кви про кво» с целью получения конфиденциальных данных. Злоумышленник создает вредоносное программное обеспечение (ПО) под видом программы повышающей быстродействие, осу-

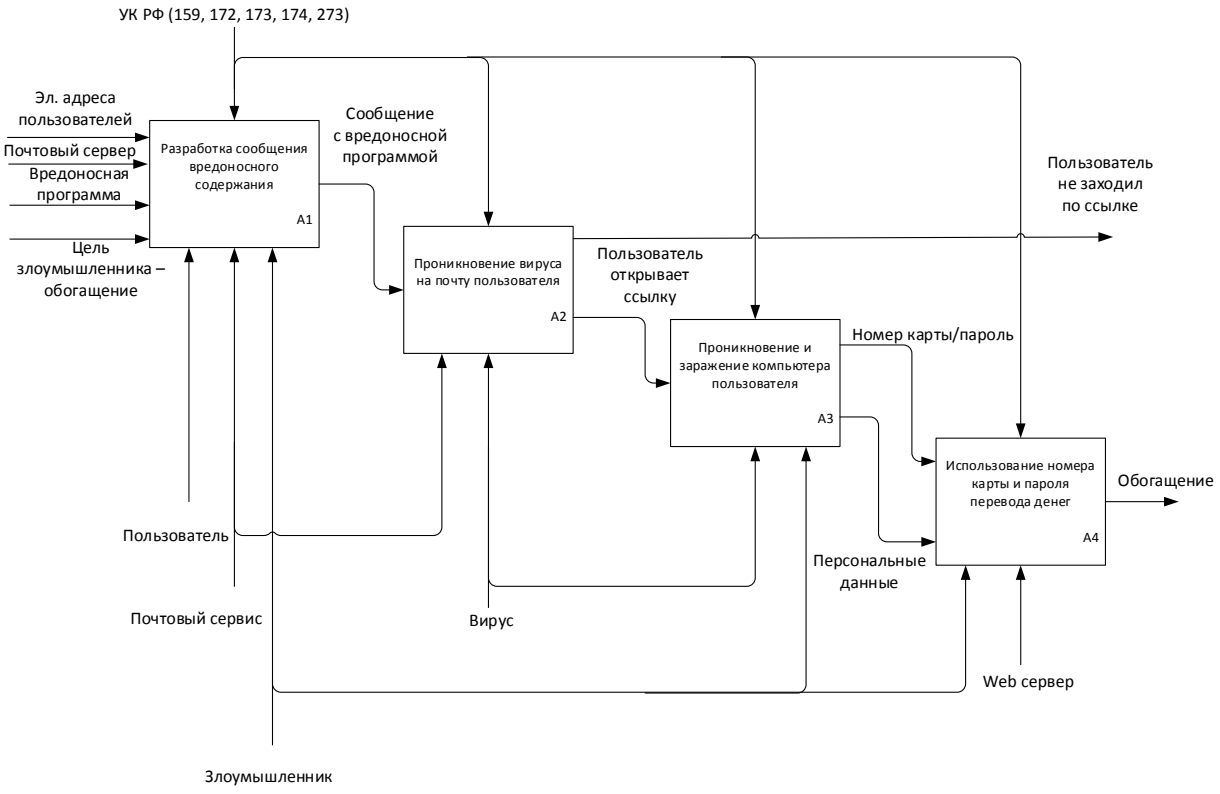

Рис. 1. *Диаграмма A0 реализации кибератаки похищения денежных средств на основе метода социальной инженерии «Фишинг»*

ществляет поиск пользователей с такой проблемой на различных ресурсах и получает его контактные данные. Связывается с пользователем и убеждает установить ПО, пользователь устанавливает вредоносное ПО, и злоумышленник получает доступ к конфиденциальным данным.

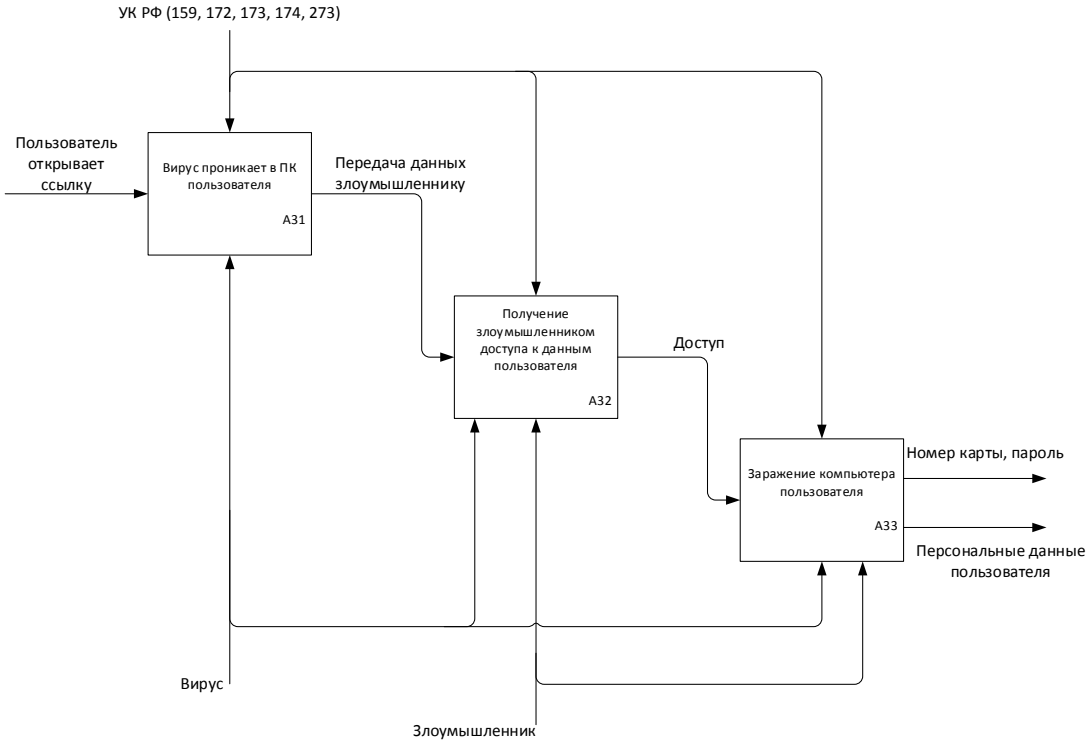

Рис. 2. *Диаграмма A3 реализации кибератаки похищения денежных средств на основе метода социальной инженерии «Фишинг»*

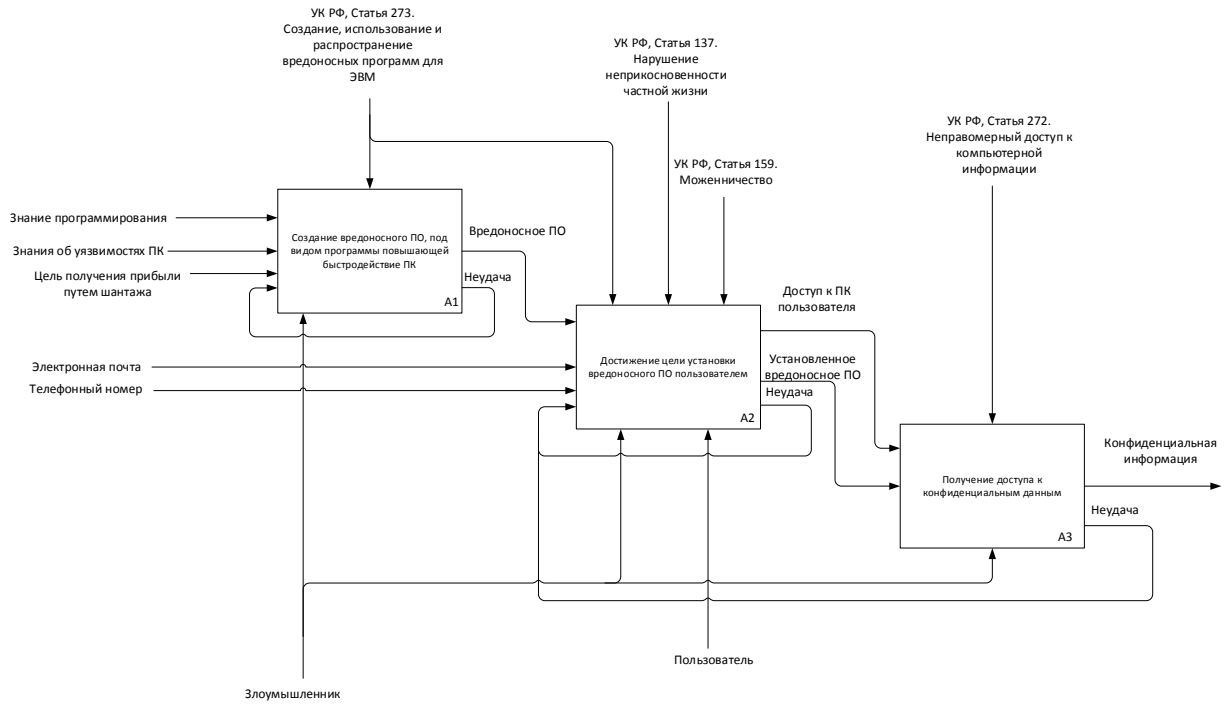

Рис. 3*. Диаграмма A0 реализации кибератаки хищения конфиденциальных данных на основе метода социальной инженерии «кви про кво»*

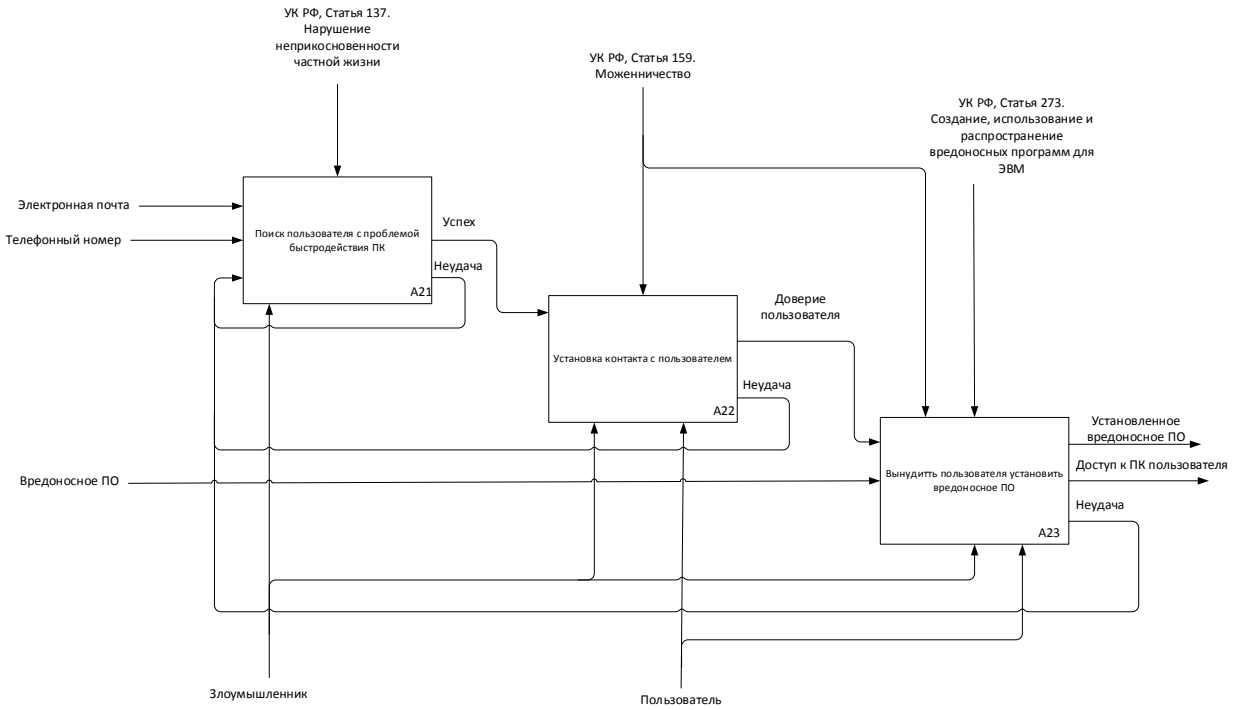

***Рис. 4**. Диаграмма A2 реализации кибератаки хищения конфиденциальных данных на основе метода социальной инженерии «кви про кво»*

На рисунках 5, 6 представлены диаграммы реализации кибератаки получения финансовых средств методами социальной инженерии. Злоумышленником разрабатывается вредоносное ПО – программа, позволяющая собирать информацию о пользователе, отправляет сообщение, содержащее ссылку на него. Запуск программы позволяет получить злоумышленнику компрометирующую информацию для шантажа пользователя. После получения нужных данных злоумышленник устанавливает связь с пользователем и средствами социальной инженерии вымогает у пользователя финансовые средства.

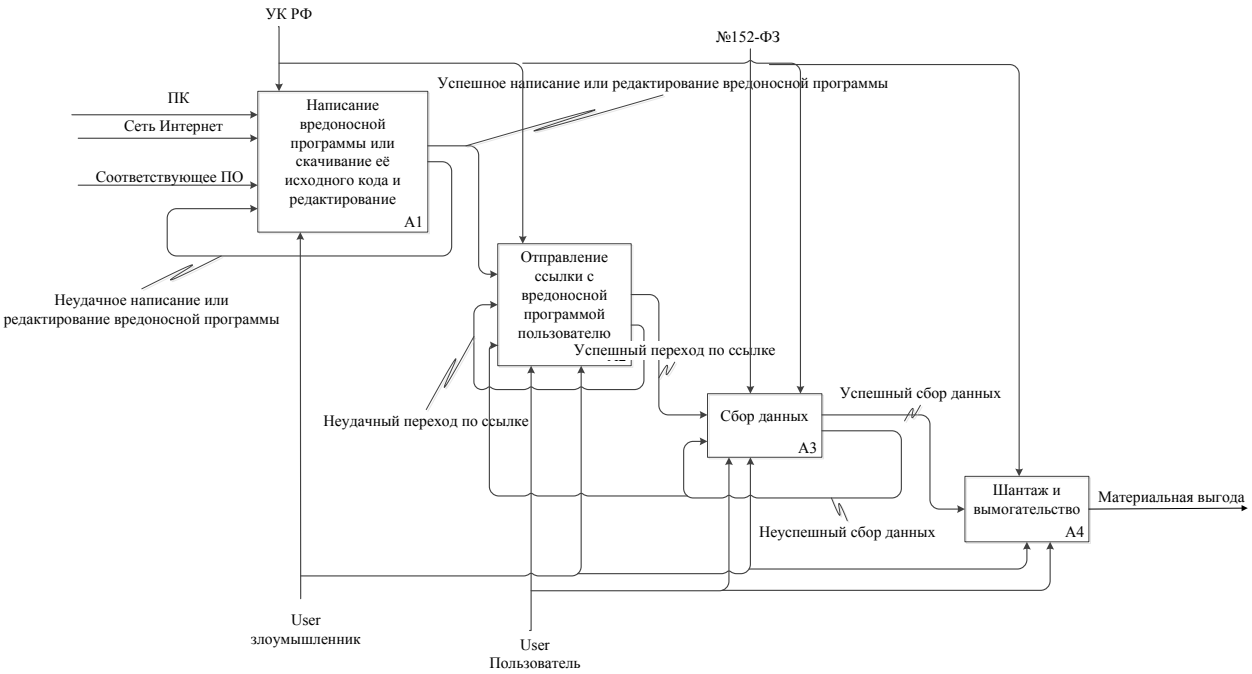

***Рис.5**. Диаграмма A0 реализации кибератаки получения финансовых средств методами социальной инженерии*

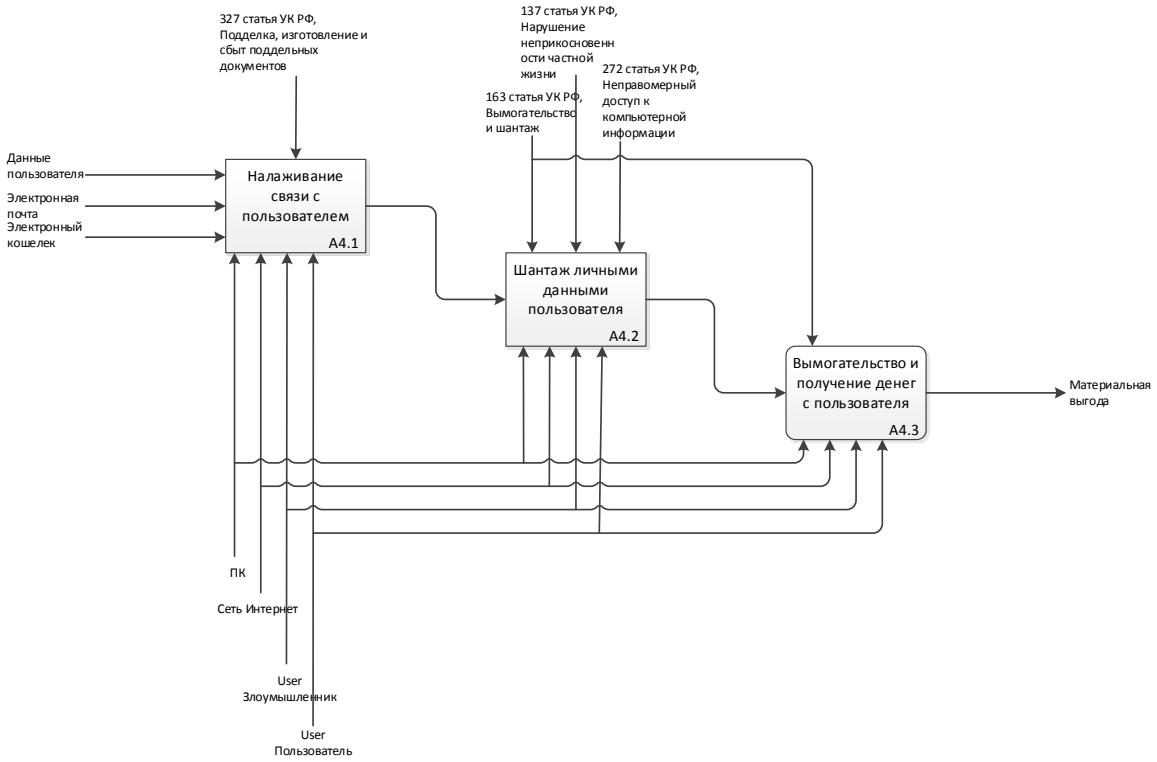

***Рис. 6**. Диаграмма A4 реализации кибератаки получения финансовых средств методами социальной инженерии*

Обобщенный алгоритм распространения таргетированной информации в ONS

В статье предложен обобщенный алгоритм распространения таргетированной информации в ONS, который можно представить в виде:

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

Алгоритм распространения таргетированной информации в ONS можно представить совокупностью исходных данных и результатов работы, которые позволят формализовать различные сценарии атак на ONS.

Совокупность исходных данных и результатов работы обобщенного алгоритма распространения таргетированной информации в ONS представлены в таблице 1.

Таблица 1
Параметры обобщенного алгоритма распространения таргетированной информации в ONS

Входные параметры $X = \{x_1, \ldots, x_j\}$ – пользователи ONS	$x_1 = \{x_1^i \mid i = \overline{1,n}\}$ – 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 социальных сетей, образование, место проживания и т.п.).

	$x_2 = \left\{x_2^j \mid j = \overline{1,m}\right\}$ – посты пользователя социальной сети	x_2^1 – количество постов, x_2^2 – количество комментариев к постам, x_2^3 – геолокация постов.
	$x_3 = \left\{x_3^\gamma \mid \gamma = \overline{1,s}\right\}$ – оценки постов и сообщений	x_3^1 – количество оценок других пользователей «мне нравится», x_3^2 – количество репостов сообщений других пользователей сообществ, x_3^3 – количество сообщений в других социальных сетях, x_3^4 – количество сообщений личного диалога пользователя.
	$x_4 = \left\{x_4^\lambda \mid \lambda = \overline{1,\beta}\right\}$ – друзья и подписчики	x_4^1 – количество подписчиков пользователя, x_4^1 – количество друзей пользователя;
	$x_5 = \left\{x_5^\sigma \mid \sigma = \overline{1,p}\right\}$ – профиль страницы пользователя	x_5^1 – закрытый профиль, x_5^2 – открытый профиль.
	$x_6 = \left\{x_6^k \mid k = \overline{1,\tau}\right\}$ – посты	x_6^1 – количество постов пользователя, x_6^2 – ссылки на собственные сайты, другие социальные сети, x_6^3 – количество репостов.
	$x_7 = \left\{x_7^d \mid d = \overline{1,w}\right\}$ – цель злоумышленника	x_7^1 – финансовая выгода, x_7^2 – самоутверждение перед самим собой, x_7^3 – самоутверждение перед лицом какого-либо сообщества/общества социальной сети, 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.
Параметры внутренних состояний алгоритма $Z = \left\{z_1,\ldots,z_\gamma\right\}$ – использование методов социальной инженерии пользователем ONS	$z_1 = \left\{z_1^i \mid i = \overline{1,k}\right\}$ – использование методов получения доступа к данным авторизации	z_1^1 – использование новых уязвимостей социальной сети и различных протоколов передачи данных, z_1^2 – использование известных уязвимостей и протоколов передачи данных, z_1^3 – распространение ссылок на сайты, содержащие известные вредоносные программы, z_1^4 – распространение копий известных вредоносных программ, z_1^5 – распространение ссылок на сайты, содержащие новые самописные вредоносные программы, z_1^6 – распространение копий новых самописных вредоносных программ, z_1^7 – распространение ссылок на фишинговые сайты,

		z_1^8 – использование атаки прямого перебора, z_1^9 – использование атаки по словарю, z_1^{10} – использование радужных таблиц, z_1^{11} – взлом аккаунта пользователя, z_1^{12} – взлом почтового ящика пользователя, z_1^{13} – кража 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.
	$z_2 = \left\{ z_2^{\chi} \mid \chi = \overline{1,s} \right\}$ – 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 социальной сети под предлогом распространения благотворительной информации социальной направленности, z_2^8 – установление договоренностей с лидером социальной сети под предлогом распространения рекламной информации с последующим вознаграждением, z_2^9 – установление договоренностей с лидером ONS для распространения информации, апеллируя к иным скрытым мотивам (самоутверждение, обладание информацией).
	$z_3 = \left\{ z_3^{\tau} \mid \tau = \overline{1,\omega} \right\}$ – 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 ONS 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 ONS для распространения информации, апеллируя к иным скрытым мотивам (нематериальная выгода, самоутверждение, осведомленность) [12 – 13].
Выходные параметры: $Y = \{y_1,..., y_p\}$ – реализованные цели злоумышленника	y_1^1 – материальный интерес, y_1^2 – самоутверждение перед самим собой, y_1^3 – самоутверждение перед лицом сообщества/общества, y_1^4 – месть знакомым, y_1^5 – месть сообществу, y_1^6 – месть мировой системе, y_1^7 – месть предприятию-работодателю, y_1^8 – преимущество в конкурентной борьбе, y_1^9 – хулиганство, y_1^{10} – интерес.	

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

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

Обработка социальной информации в ситуациях распространения таргетированной информации в социальных сетях

Выборка данного исследования представляет собой 2499 пользователей социальных сетей Twitter, Facebook, ВКонтакте, являющихся модераторами (администраторами) сообществ пользователей России, в большинстве своем, молодежь в возрасте от 17 до 30 лет. Все 2499 пользователей участвовали в тестовом опросе, касающегося 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, факторы в ситуациях повышенного риска распространения нежелательной информации в социальных сетях.

В исследовании все тестовые опросы являлись анонимными и проводились в течении 6 месяцев 2016 – 2017 гг. Один тестовый опрос пользователя длился около 1 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 исследовании 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, распространения нежелательной информации и купированию их, в которых они участвовали.

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, 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». В таблице 2 приводятся статистические данные выборки из 2499 респондентов.

Средний возраст респондентов составил 22 года. Из них 74,99% мужчин – остальные женщины. Более половины, респондентов имеют законченное высшее образование (65,98%). Большинство респондентов указали на принадлежность к низшему классу (70,99%), т.к. респонденты – это студенты, основным источником которых являются стипендия и случайный заработок. Остальные респонденты относят себя к среднему классу в 26% случаев – это респонденты 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 69,03%, имеет гражданского партнера 23,97%, а в официальном браке состоят всего 7%.

В ходе исследования 2499 респондентов сообщили (табл. 2) более чем о 20 тыс. нежелательных сообщениях, поступивших от различных пользователей социальных сетей. За анализируемый промежуток времени пользователи получали от 4 до 10 сообщений, содержащих нежелательную информацию – 33,41%, 11,72% респондентов отметили, что не получали подобные сообщения. В 39,98% случаях отправителем сообщений содержащих нежелательную информацию являются неизвестных пользователей и 30,01% – с фейковых ак-

Таблица 2
Описательная статистика (со слов респондентов) выборки из 2499 пользователей социальных сетей

Переменная	Частотность	%	Переменная	Частотность	%
Половая принадлежность			**Уровень знаний в IT- сфере**		
Мужчина	1875	74,99	низкий	100	4,00
Женщина	625	25,01	средний	2025	81,03
Возраст			высокий	374	14,97
от 17 до 20 лет	450	18,01	**Принадлежность к социальной сети**		
от 20 до 24 лет	950	38,02	хобби, развлечения	548	21,93
от 24 до 27 лет	774	30,97	обучение	575	23,01
от 27 до 30 лет	200	8,00	религия	577	23,09
Более 30 лет	125	5,00	знакомства	630	25,21
Образование			проблема, беда	552	22,09
Среднее	575	23,01	бизнес	585	23,41
Начальное профессиональное	275	11,00	**Количество подписчиков в социальной сети**		
Высшее бакалавриат	1049	41,98	< 50	999	39,98
Высшее специалитет	200	8,00	50 - 100	625	25,01
Магистратура	200	8,00	100 – 200	375	15,01
Аспирантура	200	8,00	200 – 500	375	15,01
Семейное положение			> 1000	125	5,00
Холост	1725	69,03	**Количество друзей в социальной сети**		
Имею гражданского партнера	599	23,97	< 50	125	5,00
В браке	175	7,00	50 - 100	500	20,01
Финансовое положение			100 – 200	1000	40,02
низший класс	1774	70,99	200 – 500	500	20,01
средний класс	650	26,01	> 1000	374	14,97
высший класс	75	3,00			

каунтов. Реже всего такие сообщения приходят от друзей 5,00% и администраторов (модераторов) различных сообществ социальных сетей 5,00%. Данная статистика характеризуется 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 быть и принимают равные значения 15% ± 1%. Это вредоносные программы, ссылки на фишинг сайты, вербовка в террористические группы, вовлечение в сомнительные группы, спам и даже реклама товаров и услуг. 85,83% респондентов отметили, что на свои аккаунты в социальных сетях не было ни одной кибератаки, что вероятнее всего обусловлено недостаточным промежутком времени исходной выборки (6 месяцев) и, следовательно, обращений в службу технической поддержки не целесообразно – 79,79%.

Очень часто в социальных сетях пользователи просят друг другу помочь в рассылке какой-либо информации, например, призыв помощи и т.п. По статистике большинству респондентам подобного рода сообщения с просьбой о чем-либо поступала менее 5 раз (39,22%) или вовсе не приходила (13,49%). Соглашаясь на рассылку подобного рода сообщений с просьбой о чем-либо многие респонденты преследуют финансовую выгоду (71,67%) или с целью самоутверждения (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 социальных сетей. Так 77,01% респондентов отметили, что ключевых словосочетаний/слов в базе данных фильтрации сообщений составляет менее 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, привлечение администраторов (модераторов) сообществ в социальных сетях, т.к. они чаще всего обладают высоким уровнем доверия среди пользователей и вероятность достижения своих целей злоумышленником высока.

Методика защиты от распространения таргетированной информации в ONS

На основе исследования социальной информации в ситуациях распространения таргетированной информации в социальных сетях в статье предложена методика защиты от распространения таргетированной информации в ONS (рис. 7), которая представляет собой последовательность шагов:

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

Формально данную методику можно представить:

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

$X = \{x_i \mid i = \overline{1,n}\}$ – 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_0 – 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 па-

Таблица 3

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

Переменная	Частотность	%	Переменная	Частотность	%
Количество получаемых сообщений нежелательного содержания			**Количество обращений в службу технической поддержки**		
не получал	293	11,72	не обращался	1994	79,79
менее 3 раз	732	29,29	менее 5 раз	266	10,64
от 4 до 10 раз	835	33,41	от 5 до 20 раз	204	8,16
от 11 до 15 раз	328	13,13	от 20 до 30 раз	35	1,40
от 16 до 20 раз	210	8,40	от 30 до 50 раз	0	0,00
более 20 раз	101	4,04	более 50 раз	0	0,00
Кто является отправителем сообщений нежелательного содержания в социальной сети			**Количество обращений к модератору (администратору) социальной сети для блокировки определенного пользователя**		
пользователи сообществ социальной сети	500	20,01	не обращался	1637	65,51
модератор (администратор) социальной сети	125	5,00	менее 5 раз	676	27,05
фейковый аккаунт	750	30,01	от 5 до 20 раз	142	5,68
друг	125	5,00	от 20 до 30 раз	0	0,00
неизвестный пользователь	999	39,98	от 30 до 50 раз	44	1,76
Содержание сообщений нежелательного содержания			более 50 раз	0	0,00
ссылка на вредоносный код	343	13,73	**Сколько раз вам поступали предложения, как модератору (администратору) сообщества социальной сети сделать рассылку информационных сообщений нежелательного содержания пользователям вашего сообщества**		
ссылка на фишинг сайт	404	16,17	не поступали	337	13,49
вовлечение в террористические группы	362	14,49	менее 5 раз	980	39,22
вовлечение в сомнительные группы	372	14,89	от 5 до 20 раз	690	27,61
спам	377	15,09	от 20 до 30 раз	152	6,08
реклама товаров, услуг	369	14,77	от 30 до 50 раз	171	6,84
Количество кибератак на Ваш аккаунт			более 50 раз	169	6,76
нет	2145	85,83			
менее 3 раз	353	14,13			
от 4 до 10 раз	1	0,04			
от 11 до 15 раз	0	0,00			
более 15 раз	0	0,00			
Достигли ли вы своей цели, путем распространения нежелательной информации согласившись на рассылку информационных сообщений			**Сколько ключевых словосочетаний/слов в базе данных сообщества (где вы являетесь модератором) для фильтрации сообщений**		
да	1646	65,87	менее 10	250	77,01
нет	516	20,65	от 10 до 15	249	9,96
Сколько раз Вы обращались в службу технической поддержки с просьбой заблокировать аккаунт пользователя, распространяющего нежелательную информацию			от 15 до 20	500	10,01
не обращался	250	10,00	более 20	1500	3,02
менее 5 раз	874	34,97			
от 5 до 20 раз	1000	40,02			
от 20 до 30 раз	250	10,00			
более 30 раз	125	5,00			

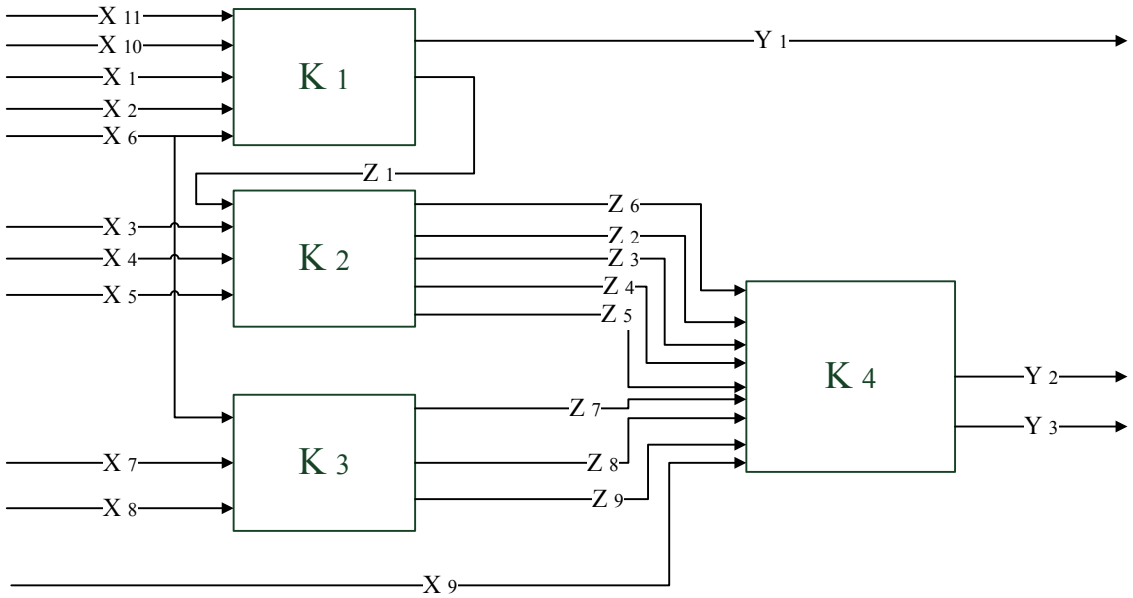

Рис. 7. *Структурная схема методики защиты от таргетированной информации*

раметров 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 ONS» включает:

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

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

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

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

Функциональный блок «Защита лидеров ONS» включает:

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

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

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

1) формирование базы данных сообщений пользователей, содержащих таргетированную информацию, распространяемую в ONS на основе анализа данных заблокированных пользователей;
2) разработка критериев оценивания информации сообщений пользователей;
3) формирование базы правил классифика-

ции 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 социальных сетей.

Функциональный блок «Выработка рекомендаций по защите от таргетированной информации в ONS» декомпозируется на 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 распространённые социальные сети, а пользователям повысить безопасность использования личной информации в социальных сетях и не попадаться на уловки злоумышленников. Предполагается, что специальное программное обеспечение будет представлять собой программный модуль – приложение, позволяющее:

- фильтровать личные сообщения пользователей, сообщений-записей (постов) пользователей сообществ социальных сетей на основе модели фильтрации сообщений;
- в автоматизированном режиме блокировать пользователей, рассылающих нежелательную информацию на основе образов злоумышленников, базы правил о блокировании пользователей;
- предоставлять рекомендации администраторам (модераторам) социальных сетей о возможных угрозах реализации атак злоумышленниками и принятии контрмер по предотвращению кибератак в социальных сетях.

Исследования в этом направлении будут продолжены.

Заключение

Предложенная в статье методика защиты от таргетированной информации в виртуальных социальных сетях позволит предотвратить угрозы информационной безопасности, предотвратить попытки злоумышленников реализации социоинженерных атак, разработать модель защиты от таргетированной информации и в дальнейшем реализовать специальное программное обеспечение для его интегрирования в системы Online Social Network. Все это позволит проводить внешний мониторинг событий в ONS, а также осуществлять поиск уязвимостей в механизмах обмена мгновенными сообщениями для возможности реализации атак злоумышленниками, защите личной информации пользователей социальных сетей. Результаты исследования позволяют на новом уровне применять активно развивающийся сегодня сетевой подход к исследованию неформальных сообществ, получая интересные и наглядные результаты.

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им. Н.Э. Баумана. E-mail: v.tsirlov@cnpo.ru*

Литература:

1. Тультаева И.В., Каптюхин Р.В., Тультаев Т.А. Воздействие социальных сетей на коммуникационные процессы в современном обществе // Бизнес. Образование. Право. Вестник Волгоградского института бизнеса. 2014. № 4. С. 84-88.
2. Ревенков П.В. Электронные деньги: источники рисков при использовании в противоправных целях // Национальные интересы: приоритеты и безопасность. 2016. № 1 (334). С. 164-175.
3. Маркелова А.В., Козырева В.А., Сметанина О.Н. Модели управления процессом реализации академической мобильности в ВУЗе // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2011. Т. 9. № 2. С. 55-65.
4. Мурзин Ф.А., Батура Т.В., Проскуряков А.В. Программный комплекс для анализа данных из социальных сетей // Программные продукты и системы. 2015. № 4 (112). С. 188-197.
5. Майдыков А.А., Исаров О.Б. Национальные интересы - актуальные проблемы противодействия использованию интернета террористическими и экстремистскими организациями // Национальные интересы: приоритеты и безопасность. 2015. № 38 (323). С. 44-51.

6. Юсупова Н.И., Ризванов Д.А., Сметанина О.Н., Еникеева К.Р. Модели представления знаний для поддержки принятия решений при управлении сложными системами в условиях неопределенности и ресурсных ограничений. В сборнике: Information Technologies for Intelligent Decision Making Support (ITIDS'2016) Proceedings of the 4th International Conference. 2016. С. 24-27.
7. Юсупова Н.И., Сметанина О.Н., Еникеева К.Р. Иерархические ситуационные модели для сппр в сложных системах // Современные проблемы науки и образования. 2013. № 4. С. 63.
8. 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.
9. Мирзануров Д.Х. Методика защиты от нежелательной информации, распространяемой в системах Social Network // Символ науки. 2015. № 5. С. 48-51.
10. Козырь Н.С., Мальков А.А. Корпоративная культура как элемент национальной безопасности государства // Национальные интересы: приоритеты и безопасность. 2015. № 44. С. 53-66.
11. Кузнецов Д.А. Зависимость экономической и военной безопасности России от состояния защищенности стратегически важных объектов // Национальные интересы: приоритеты и безопасность. 2015. № 17 (302). С. 52- 60.
12. Федоров П. ВКонтакте опережает Instagram по числу зарегистрированных пользователей [Электронный ресурс] – http://siliconrus.com/2014/01/vkontakte-operezhaet-instagram-po-chislu-zaregistrirovannyih-polzovateley/ [Дата обращения: 21.09.2016].
13. Eset: аккаунты соцсетей 60% пользователей рунета взламывались хакерами [Электронный ресурс] – http://www.securitylab.ru/news/442581.php [Дата обращения: 21.09.2016].
14. Мирзабалаева Ф.И., Алиева П.Р. Безопасное развитие кадрового потенциала проблемного региона // Национальные интересы: приоритеты и безопасность. 2015. № 21. С. 56-66.
15. Яшников А.Ю., Болодурина И.П. Выявление лидеров мнений социальной сети // Молодежный научный форум: технические и математические науки. 2016. № 5 (34). С. 59-65.
16. Smetanina O.N., Maximenko Z.V., Klimova A.V. Models of education quality estimation based on fuzzy classification // Вестник Уфимского государственного авиационного технического университета. 2013. Т. 17. № 6. С. 53-56.
17. Тумбинская М.В., Сафиуллина А.М. Программное обеспечение оценивания тестовых заданий для выявления компетенций кадрового резерва с элементами защиты информации // Национальные интересы: приоритеты и безопасность. 2012. № 35. С. 42-47.
18. Царегородцев А.В., Макаренко Е.В. Методика количественной оценки риска в информационной безопасности облачной инфраструктуры организации // Национальные интересы: приоритеты и безопасность. 2014. № 44 (281). С. 30-41.
19. Юсупова Н.И., Шахмаметова Г.Р. Интеграция инновационных информационных технологий: теория и практика // Вестник Уфимского государственного авиационного технического университета. 2010. Т. 14. № 4 (39). С. 112-118.

SYSTEM APPROACH TO PROTECTION AGAINST UNWANTED INFORMATION IN THE SOCIAL NETWORKS

M. Tumbinskaya [2]

The targets of the study in this work are such social networks as Twitter, Facebook, Vkontakte under the conditions of the information security threats. The paper presents an algorithm for disseminating targeted information in the social networks, defines its parameters, which variety will be able to present details about various scripts of computer attacks, and suggests an innovative classification of the information security threats. Based on the study of social information, a method of protection against targeted information that is disseminated in social networks was developed. It was concluded that presentation of details of the attack scripts allowed for developing relevant counter measures. It was substantiated that the methods of protection against targeted information disseminated in the social networks allowed for developing a model of protection from targeted information and introducing special software for its integration into social networks.

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

References:

1. Tul'taeva I.V., Kaptyukhin R.V., Tul'taev T.A. Vozdeystvie sotsial'nykh setey na kommunikatsionnye protsessy v sovremennom obshchestve, Biznes. Obrazovanie. Pravo. Vestnik Volgogradskogo instituta biznesa. 2014. No 4, pp. 84-88.
2. Revenkov P.V. Elektronnye den'gi: istochniki riskov pri ispol'zovanii v protivopravnykh tselyakh, Natsional'nye interesy: prioritety i bezopasnost'. 2016. No 1 (334), pp. 164-175.

2 Marina Tumbinskaya, Ph.D., Kazan National Research Technical University after A.N.Tupolev-KAI, Kazan, tumbinskaya@inbox.ru

3. Markelova A.V., Kozyreva V.A., Smetanina O.N. Modeli upravleniya protsessom realizatsii akademicheskoy mobil'nosti v VUZe, Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Informatsionnye tekhnologii. 2011. T. 9. No 2, pp. 55-65.
4. Murzin F.A., Batura T.V., Proskuryakov A.V. Programmnyy kompleks dlya analiza dannykh iz sotsial'nykh setey, Programmnye produkty i sistemy. 2015. No 4 (112), pp. 188-197.
5. Maydykov A.A., Isarov O.B. Natsional'nye interesy - aktual'nye problemy protivodeystviya ispol'zovaniyu interneta terroristicheskimi i ekstremistskimi organizatsiyami, Natsional'nye interesy: prioritety i bezopasnost'. 2015. No 38 (323), pp. 44-51.
6. Yusupova N.I., Rizvanov D.A., Smetanina O.N., Enikeeva K.R. Modeli predstavleniya znaniy dlya podderzhki prinyatiya resheniy pri upravlenii slozhnymi sistemami v usloviyakh neopredelennosti i resursnykh ogranicheniy. V sbornike: Information Technologies for Intelligent Decision Making Support (ITIDS'2016) Proceedings of the 4th International Conference. 2016, pp. 24-27.
7. Yusupova N.I., Smetanina O.N., Enikeeva K.R. Ierarkhicheskie situatsionnye modeli dlya sppr v slozhnykh sistemakh, Sovremennye problemy nauki i obrazovaniya. 2013. No 4, p. 63.
8. Nazarov A.N., Galushkin A.I., Sychev A.K. Risk-modeli i kriterii informatsionnogo protivoborstva v sotsial'nykh setyakh, T-Comm: Telekommunikatsii i transport. 2016. T. 10. No 7, pp. 81-86.
9. Mirzanurov D.Kh. Metodika zashchity ot nezhelatel'noy informatsii, rasprostranyaemoy v sistemakh Social Network, Simvol nauki. 2015. No 5, pp. 48-51.
10. Kozyr' N.S., Mal'kov A.A. Korporativnaya kul'tura kak element natsional'noy bezopasnosti gosudarstva, Natsional'nye interesy: prioritety i bezopasnost'. 2015. No 44, pp. 53-66.
11. Kuznetsov D.A. Zavisimost' ekonomicheskoy i voennoy bezopasnosti Rossii ot sostoyaniya zashchishchennosti strategicheski vazhnykh ob"ektov, Natsional'nye interesy: prioritety i bezopasnost'. 2015. No 17 (302), pp. 52- 60.
12. Fedorov P. VKontakte operezhaet Instagram po chislu zaregistrirovannykh pol'zovateley [Elektronnyy resurs] – http://siliconrus.com/2014/01/vkontakte-operezhaet-instagram-po-chislu-zaregistrirovannyih-polzovateley/ [Data obrashcheniya: 21.09.2016].
13. Eset: akkaunty sotssetey 60% pol'zovateley runeta vzlamyvalis' khakerami [Elektronnyy resurs] – http://www.securitylab.ru/news/442581.php [Data obrashcheniya: 21.09.2016].
14. Mirzabalaeva F.I., Alieva P.R. Bezopasnoe razvitie kadrovogo potentsiala problemnogo regiona, Natsional'nye interesy: prioritety i bezopasnost'. 2015. No 21, pp. 56-66.
15. Yashnikov A.Yu., Bolodurina I.P. Vyyavlenie liderov mneniy sotsial'noy seti, Molodezhnyy nauchnyy forum: tekhnicheskie i matematicheskie nauki. 2016. No 5 (34), pp. 59-65.
16. Smetanina O.N., Maximenko Z.V., Klimova A.V. Models of education quality estimation based on fuzzy classification, Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2013. T. 17. No 6, pp. 53-56.
17. Tumbinskaya M.V., Safiullina A.M. Programmnoe obespechenie otsenivaniya testovykh zadaniy dlya vyyavleniya kompetentsiy kadrovogo rezerva s elementami zashchity informatsii, Natsional'nye interesy: prioritety i bezopasnost'. 2012. No 35, pp. 42-47.
18. Tsaregorodtsev A.V., Makarenko E.V. Metodika kolichestvennoy otsenki riska v informatsionnoy bezopasnosti oblachnoy infrastruktury organizatsii, Natsional'nye interesy: prioritety i bezopasnost'. 2014. No 44 (281), pp. 30-41.
19. Yusupova N.I., Shakhmametova G.R. Integratsiya innovatsionnykh informatsionnykh tekhnologiy: teoriya i praktika, Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2010. T. 14. No 4 (39), pp. 112-118.