УДК 004.056.53

М.В. Абрамов

АВТОМАТИЗАЦИЯ АНАЛИЗА СОЦИАЛЬНЫХ СЕТЕЙ ДЛЯ ОЦЕНИВАНИЯ ЗАЩИЩЁННОСТИ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК [1]

Абрамов Максим Викторович, *окончил математико-механический факультет Санкт-Петербургского государственного университета, младший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук. Старший преподаватель кафедры информатики Санкт-Петербургского государственного университета. Имеет монографии, учебные пособия, статьи в области информационной безопасности и социоинженерных атак, свидетельства о регистрации программ для ЭВМ. [e-mail: mva16@list.ru].*

Аннотация

В статье представлена концепция программного комплекса автоматизированной системы анализа защищённости пользователей компьютерных сетей от социоинженерных атак. Приведена архитектура прототипа программного комплекса, изложены подходы к построению алгоритмов для модулей, отвечающих за моделирование распространения социоинженерной атаки на социальном графе сотрудников и восстановление метапрофиля пользователя на основании контента, публикуемого в социальных сетях. Представлен подход к построению и анализу социального графа сотрудников, дана критическая оценка разработанных ранее методов. Представлен алгоритм для вывода коэффициентов дуг социального графа, используемых при расчёте вероятности успеха опосредованной социоинженерной атаки.

Ключевые слова: информационная безопасность, социоинженерные атаки, защита пользователя, социальный граф сотрудников компании, метапрофиль пользователя, профиль уязвимостей пользователя.

AUTOMATION OF THE SOCIAL NETWORKS WEBSITES CONTENT ANALYSIS IN THE PROBLEMS OF FORECASTING THE PROTECTION OF THE INFORMATION SYSTEMS USERS FROM SOCIAL ENGINEERING ATTACKS

Maksim Viktorovich Abramov, *graduated from the Faculty of Mathematics and Mechanics of St. Petersburg State University; a junior researcher at the Laboratory for Theoretical and Interdisciplinary Problems of Informatics at St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Senior Lecturer of the Department of Informatics of St. Petersburg State University; an author of monographs, textbooks, articles in the field of information security and social engineering attacks; a holder of certificates of registration of computer programs. e-mail: mva16@list.ru.*

Abstract

This article deals with a software application concept of an automated system for analyzing the protection of online users from social engineering attacks. The architecture of software application prototype is presented. Approaches to algorithm development for the modules responsible for the social engineering attack spread simulation on the social graph of employees and the restoration of the user meta profile on the basis of content published in social networks are proposed. An approach to the building and analyzing of the social graph of employees is presented. The existing methods are evaluated with a critical eye. The algorithm for placing the coefficients on the arcs of the social graph used when calculating success probability of an indirect social engineering attack is presented.

Key words: information security, social engineering attacks, user protection, social graph of company employees, user meta profile, user's vulnerabilities profile.

1 Работа выполнена в рамках проекта по государственному заданию СПИИРАН № 0073-2014-0002 при финансовой поддержке РФФИ (проект № 16-31-00373 Методы идентификации параметров социальных процессов по неполной информации на основе вероятностных графических моделей).

Введение

Ускоряющаяся и расширяющаяся, причем далеко не планово и не системно, информатизация общества существенно повышает актуальность вопросов информационной безопасности (ИБ) информационных систем, причем эти системы становятся более уязвимы к кибератакам, что связано с существенным ростом частоты и сложности последних [1–5]. Вместе с тем также растут и убытки от киберпреступлений, время, затрачиваемое на расследования подобных преступлений, затраты на устранение последствий [6].

Большая часть исследований в области ИБ сегодня посвящена защите от программно-технических атак. В этой области получены результаты, позволяющие минимизировать вероятность успеха атаки, сократить время на расследование преступления, производить анализ защищённости системы [7–9]. В то же время пользователь информационной системы остаётся одним из её самых уязвимых мест [6, 10]. Как бы хорошо не была защищена инфраструктура, персонал может преднамеренно или непреднамеренно её компрометировать. Атаки, использующие манипулятивные и иные техники для воздействия на пользователя с целью достижения желаемого результата, например нарушения конфиденциальности критичного документа, называются социоинженерными [10]. В настоящее время отсутствуют стандартизованные методики обеспечения защиты пользователей информационной системы от социоинженерных атак, расследования таких преступлений, анализа защищённости от социоинженерных атак. Однако необходимость в таких средствах назрела и отмечается не только профессиональным сообществом [11, 12], но и подтверждается большим количеством освещаемых в СМИ инцидентов [6, 13, 14].

Ключевым моментом как разработки методик, так и анализа защищенности пользователей от социоинженерных атак, а также бэктрекинга атак является сбор и систематизация вместе с последующими разработкой, пополнением и обновлением формальных представлений сведений об уязвимостях пользователя, его социальных связях, доступе к критичным документам, возможных атакующих воздействиях, компетенциях злоумышленника и ряда других аспектов [10]. Кроме того, указанные операции должны быть автоматизированы, то есть обеспечены соответствующим набором программных инструментов – комплексом программ.

Таким образом, актуальной видится общая цель направления исследования, заключающаяся в разработке автоматизированной системы анализа защищённости пользователей компьютерных сетей от социоинженерных атак, комплекса упреждающей диагностики и бэктрекинга. Частная цель, достигаемая в данной статье, заключается в формировании концепции программного комплекса для оценки защищённости пользователей информационных систем от социоинженерных атак, конструировании архитектуры этого программного комплекса, построении алгоритмов для модулей, отвечающих за моделирование распространения социоинженерной атаки на социальном графе сотрудников и восстановление метапрофиля пользователя на основании контента, публикуемого в социальных сетях. Детализация части представленных в концепции моделей нашла отражение в более ранних публикациях [15–17].

Архитектура автоматизированной системы анализа защищённости пользователей компьютерных сетей от социоинженерных атак

Разрабатываемый комплекс предполагает распределённую систему модулей, каждый из которых решает некоторую задачу и посредством API-интерфейсов получает и передаёт необходимые данные в ядро. Архитектура комплекса представлена на рисунке 1. Модуль Workers Graph отвечает за поиск аккаунтов сотрудников компании в социальной сети ВКонтакте (https://vk.com/) [15]. Модуль Psychological traits предназначен для анализа публикуемого в социальных сетях контента поль-

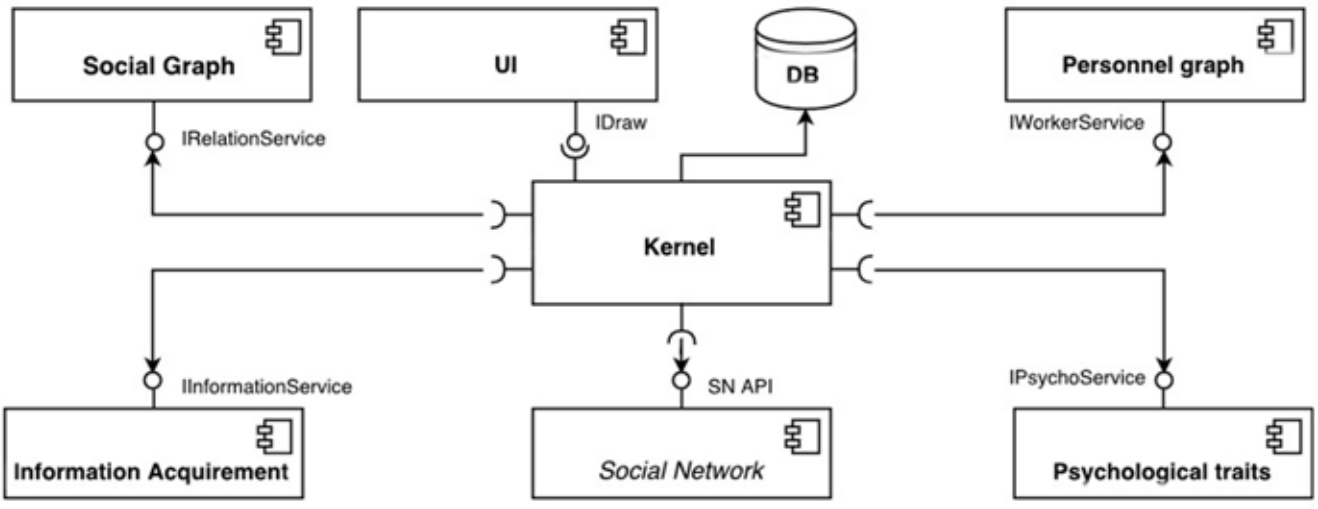

Рис. 1. Диаграмма компонент комплекса программ для оценки защищённости персонала информационной системы

зователей информационных систем и построения на их основе профиля уязвимостей [18]. В данной статье более подробно будут рассмотрены модули Social Graph и Information Acquirement. Первый предназначен для построения оценок успешности опосредованных социоинженерных атак, т. е. таких, при которых атакующее воздействие на пользователя происходит через других пользователей. Второй модуль предназначен для восстановления метапрофиля пользователя по контенту, публикуемому в социальных сетях.

Распространение социоинженерного атакующего воздействия злоумышленника на пользователей

Распространение социоинженерного атакующего воздействия может зависеть от разных факторов, таких как права доступа сотрудников, внутренняя архитектура офиса, характер взаимоотношений в компании [10]. В данном материале сосредоточимся на последнем – характере взаимоотношений между сотрудниками. Чтобы определить, в каких отношениях состоят сотрудники компании, предлагается использовать их аккаунты в социальных сетях. Для этого построим социальный граф, в котором на рёбрах обозначим веса, характеризующие вероятность успеха прохождения социоинженерной атаки по данной связи.

Для построения социального графа взаимодействия будем основываться на открытой информации, полученной из профилей в социальной сети ВКонтакте. Обоснование данного подхода связано в том числе с тем, что к этой информации может получить доступ и злоумышленник, следовательно, учитывать её при планировании атаки. Также отметим, что информация, публикуемая пользователем в социальной сети, как правило, больше соответствует действительности, чем получаемая в рамках опросов или интервью [19].

Опытный злоумышленник-социоинженер, основываясь на информации, полученной из социальных сетей, может сделать выводы, которые будут способствовать успеху проводимой им атаки [20]. Так, например, доверчивый сотрудник уязвим к убеждению и обману, сильно любопытный сотрудник может попасться на уловки, использующие его интерес для создания рычагов давления. Информацию о таких и других личностных особенностях злоумышленник может извлечь из аккаунта в социальной сети и использовать в своих целях [21]. При этом становится понятен круг общения потенциальной жертвы. Можно предположить, что чем теснее общаются между собой коллеги, тем вероятнее успех прохождения социоинженерной атаки на одного через другого. Положение усугубляется, если среди сотрудников компании есть инсайдер, заинтересованный в компрометации системы, поскольку он, как правило, обладает информацией о характере взаимоотношений коллег, правах доступа, сам общается с кем-то из коллег. Всё это существенно облегчает атаку и повышает вероятность её успеха.

Для представления в форме математической модели характера взаимоотношений сотрудников предлагается построить социальный граф компании. Множество вершин данного социального графа будет определяться множеством сотрудников компании, множество рёбер – связями между сотрудниками в компании. Изначально строится полный двунаправленный граф, где между любыми двумя сотрудниками есть ребро. Далее на рёбрах определяются весовые коэффициенты. Для определения весовых коэффициентов используются данные, получаемые из социальной сети ВКонтакте. Алгоритм присвоения коэффициентов представлен на рисунке 2.

В более ранних публикациях алгоритмы анализа вероятности успешности осуществления атаки на пользователя сводили к произведению коэффициен-

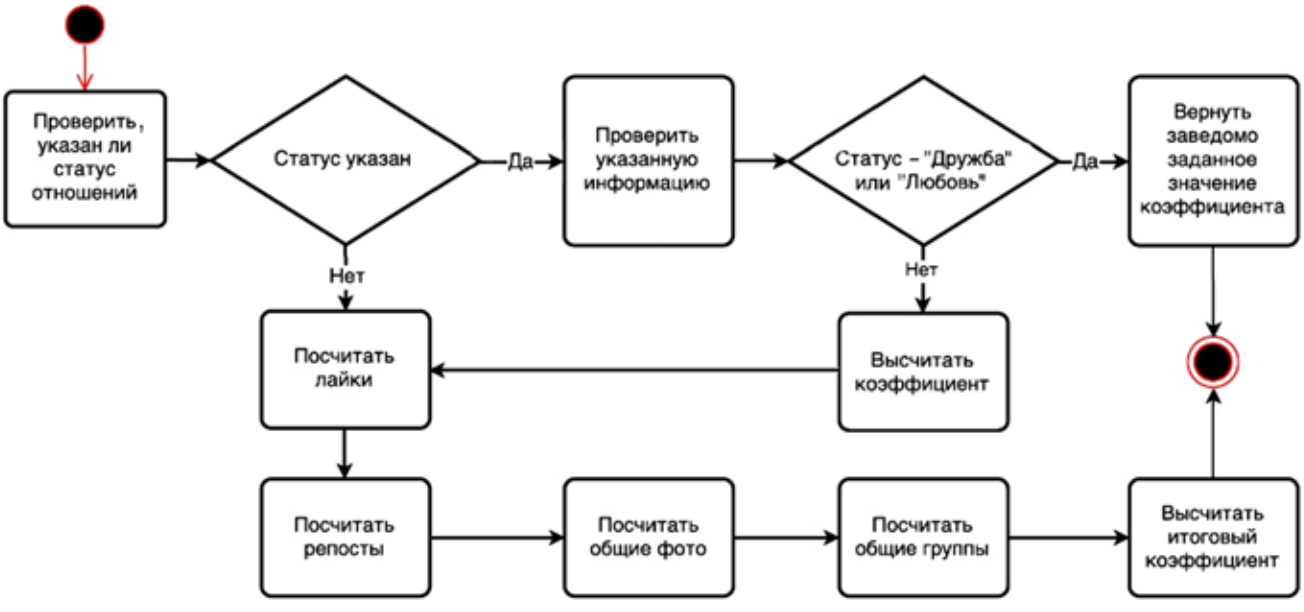

Рис. 2. Алгоритм расстановки весовых коэффициентов на социальном графе сотрудников

тов на ребрах графа и вероятностей успешной атаки на пользователя по каждой конкретной цепочке [10, 16, 22]. Очевидно, что в таком случае вероятность прямой атаки на пользователя (если она возможна) выше, чем аналогичных опосредованных (т. е. таких, при которых внедрение в информационную систему компании злоумышленником происходит с использованием более чем одного сотрудника компании). Это не всегда отражает действительность, т. к. при высокой степени доверия между коллегами вероятность успеха прохождения атаки через эту связь и последующей компрометации системы может быть достаточно высокой. Указанное соображение позволит принять во внимание подход, согласно которому весовые коэффициенты на рёбрах социального графа будут отражать характер взаимоотношений между сотрудниками.

Обработка полученного полного графа представляется достаточно ресурсоёмкой даже для небольшой компании. Хранение и обработка такого графа требует больших затрат памяти и лишней работы процессора (overhead). Одним из возможных решений может быть сокращение количества дуг путем исключения маловероятных путей организации социоинженерных атак. Т. е. предлагается использовать пороговое значение весового коэффициента для принятия решения – оставлять или нет ребро в графе. Таким образом получим разбиения графа на компоненты сильной связности, которые намного проще обрабатывать в рамках моделирующих процессов.

Таким образом, полученная модель позволит агрегировать большее число факторов, влияющих на успех социоинженерной атаки. Это позволит скорректировать оценки вероятности успешности атаки злоумышленника на пользователей информационной системы.

Отметим также, что в полученных компонентах связности социального графа компании с весовыми коэффициентами на рёбрах можно выделить центральные узлы, которые будут являться неформальными лидерами. В данном случае стоит учесть, что меры центральности могут быть разными в зависимости от того, какой тип лидерства требуется учесть. Неформальные лидеры в контексте социоинженерных атак обычно обладают наибольшим потенциалом для совершения атаки злоумышленником – они, зачастую, владеют наиболее полной информацией и наибольшими в коллективе возможностями по распространению атаки. Таким образом, атака через подобного «центрального пользователя» может нанести существенный ущерб компании.

Восстановление метапрофиля пользователя на основании контента из социальных сетей

Как правило, сегодня пользователь имеет аккаунты в разных социальных сетях [23]. При этом нередко в каждом из аккаунтов какая-то часть информации не представлена, какая-то не является корректной. С учетом указанных обстоятельств актуальной видится задача восстановления недостающих или недостоверных данных на основании контента, публикуемого в социальных сетях. Анкетные данные пользователя будем называть метапрофилем пользователя информационной системы. Для восстановления метапрофиля пользователя предлагается использовать два источника данных. Первый – информация из аккаунтов этого пользователя в других социальных сетях, второй – через анализ социального окружения пользователя (его друзей).

Для того чтобы извлечь информацию из аккаунтов пользователя в других социальных сетях, необходимо найти данные аккаунты. Задача идентификации аккаунтов пользователей социальных сетей не нова, но в текущей формулировке рассматривается впервые. Существующие подходы к её решению демонстрировали разные уровни эффективности [20, 24, 25]. Среди них особенно выделим методику, предложенную в работе [25]. В ней представлен подход к решению задачи поиска и сопоставления аккаунтов одного и того же человека в разных социальных сетях, приведена формализация, представлены методика и алгоритмы для сопоставления профилей одного и того же человека в Facebook и Twitter. Наш подход является расширением данного на большее число социальных сетей с учётом большего количества параметров. При анализе аккаунтов учитываются не только анкетные данные пользователей (Ф.И.О., место и год рождения, образование, работа, интересы, политические и религиозные взгляды и т. п.), характер их связей, но и фотоматериалы с хештегами, геолокационной информацией, отметки других пользователей; взаимная активность пользователей в виде лайков, репостов и прочих факторов.

Формальная постановка задачи может быть представлена следующим образом. Пусть есть n социальных графов с m вершинами. Необходимо найти такие $v_i^1..v_i^n : v_i^j \in V_j$, чтобы они принадлежали одному пользователю. Иными словами, нужно построить проекции из одного социального графа в другой (рис. 3). В нашей иллюстративной задаче $n = 3$.

Для выявления страниц одного и того же пользователя в разных социальных сетях в целях восстановления его метапрофиля используется методика, состоящая из следующих шагов [15].

1. Поиск аккаунтов пользователей в социальной сети Вконтакте, о которых заведомо известно, что они являются сотрудниками компании.

2. Поиск аккаунтов в социальных сетях Facebook и Instagram, потенциально ассоциированных с найденными аккаунтами пользователей в социальной сети ВКонтакте. В простейшем случае аккаунты будут привязаны друг к другу. В противном случае поиск осуществляется исходя из параметров, перечисленных выше.

3. В каждой тройке аккаунтов будут анализироваться анкетные данные (Ф.И.О., место и год рождения, образование, работа, интересы, политические и религиозные взгляды и т. п.), характер их социальных связей, фотоматериалы с хештегами, геолокационной инфор-

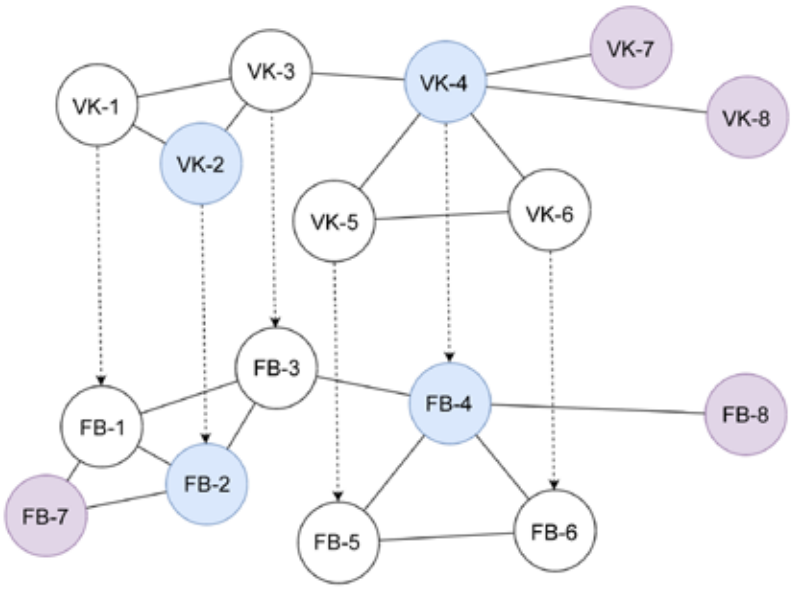

Рис. 3. Проекция из одного социального графа в другой

мацией, отметками других пользователей; взаимная активность пользователей в виде лайков, репостов и прочих факторов.

4. На основе проведённого анализа будут отсеяны тройки или элементы троек, которые были выбраны ошибочно, остальные будут включены в базу данных.

5. На основе информации из аккаунтов каждой тройки будет построен мета-профиль пользователя, содержащий более полную информацию о сотруднике компании, которая послужит базой для построения психологического профиля пользователя. Метапрофиль пользователя включает в себя анкетные данные (Ф.И.О., место и год рождения, образование, работа, интересы, политические и религиозные взгляды и т. п.).

Наряду с поиском недостающей информации в аккаунтах других социальных сетей анализируется социальное окружение пользователя в социальной сети ВКонтакте. Для этого предлагается группировать списки его друзей по различным параметрам: возрасту, школе, вузу и т. д. Предположительно, к наибольшей по численности группе в каждой категории будет относиться пользователь. Т. е., например, пользователь не указал на своей странице школу, которую окончил. Производится анализ списка его друзей, определяются пользователи, указавшие в своём аккаунте оконченную школу. Максимальная по количеству упоминаний школа считается школой, в которой учился данный пользователь.

Таким образом, мы будем иметь в лучшем случае три гипотезы по каждому пункту профиля (школа, вуз и т. д.): первая – из информации, которую пользователь сам указал о себе; вторая – из анализа аккаунтов в других социальных сетях; третья – из анализа социальных связей. В случае совпадения двух или трёх гипотез будем считать, что информация соответствует истине. Если же гипотезы не совпадают или не все представлены, то верной будем считать третью.

В результате появляется возможность оперировать большим объемом информации, за счёт чего происходит некоторое упрощение процесса извлечения психологических особенностей и последующего построения профиля уязвимостей пользователей информационной системы компании.

Заключение

В статье предложена концепция программного комплекса для оценки защищённости пользователей информационных систем от социоинженерных атак. Приведена архитектура прототипа программного комплекса, изложены подходы к построению алгоритмов для модулей, отвечающих за моделирование распространения социоинженерной атаки на социальном графе сотрудников и восстановление метапрофиля пользователя на основании контента, публикуемого в социальных сетях. Представлен подход к построению и анализу социального графа сотрудников, дана критическая оценка разработанных ранее методов. Представлен алгоритм для вывода коэффициентов дуг социального графа, используемых при расчёте вероятности успеха опосредованной социоинженерной атаки. Детализация части представленных в концепции моделей нашла отражение в более ранних публикациях [15–17].

СПИСОК ЛИТЕРАТУРЫ

1. 2012 Cost of Cyber Crime Study : United States, Ponemon Institute, October 2012. P. 30. – URL: http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_ Study_FINAL6%20.pdf.

2. 2013 Cost of Cyber Crime Study : United States, Ponemon Institute, October 2013. P. 30. – URL: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_1345 5.pdf.

3. 2014 Cost of Cyber Crime Study : United States, Ponemon Institute, October 2014. P. 30. – URL: http://resources.idgenterprise.com/original/AST-0130677_2014_US_Cost_of_ Cyber_Crime_Study_FINAL_2.pdf.

4. 2015 Cost of Cyber Crime Study : Global, Ponemon Institute, October 2015. P. 30. – URL: https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf.

5. 2016 Cost of Cyber Crime Study & the Risk of Business Innovation : Global, Ponemon Institute, October 2016. P. 37. – URL: http://www.ponemon.org/local/upload/file/2016 %20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

6. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within // Kaspersky Lab. – 2017. – URL: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (дата обращения: 06.10.2017).

7. Antonyuk E.M., Varshavsky I.E., Antonyuk P.E. Adaptive systems of automatic control with prioritized

channels // Soft Computing and Measurements (SCM) : 2017 XX IEEE International Conference on. – IEEE, 2017. – pp. 539–540.

8. Desnitsky V.A., Kotenko I.V. Modeling and analysis of security incidents for mobile communication mesh Zigbee-based network // Soft Computing and Measurements (SCM) : 2017 XX IEEE International Conference on. – IEEE, 2017. – pp. 500–502.

9. Kotenko I., Chechulin A., Branitskiy A. Generation of Source Data for Experiments with Network Attack Detection Software // Journal of Physics : Conference Series. – IOP Publishing, 2017. – Т. 820, №. 1. – P. 012033.

10. Социоинженерные атаки: проблемы анализа / А.А. Азаров, Т.В. Тулупьева, А.В. Суворова, А.Л. Тулупьев, М.В. Абрамов, Р.М. Юсупов. – СПб. : Наука, 2016 – 352 с.

11. Вконтакте выплатила пользователям более $70 тысяч за поиск уязвимостей // Новости Mail.ru. – URL: https://news.mail.ru/economics/25792158/ (дата обращения: 12.12.2017).

12. Как защитить внутреннюю сеть и сотрудников компании от атак, основанных на использовании социотехники // Microsoft. – 2007. – URL: https://technet.microsoft.com/ru-ru/library/cc875841.aspx (дата обращения: 12.12.2017).

13. Аношин И. Карточные слабости. Как не стать жертвой высокотехнологичных мошенников // РБК. Газета № 164. – URL: http://www.rbc.ru/newspaper/2017/09/29/59ca447 b9a79474aa6f65673.

14. Митник К.Д., Саймон В.Л. Искусство обмана. – М. : Компания АйТи, 2004. – 416 с.

15. Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities / N. Shindarev, G. Bagretsov, M. Abramov, T. Tulupyeva, A. Suvorova // Advances in Intelligent Systems and Computing. Proceedings of the Second International Scientific Conference “Intelligent Information Technologies for Industry” (IITI’17). 2017. Vol. 1. pp. 441–447.

16. Абрамов М.В., Азаров А.А. Анализ распространения имитированной социоинженерной атаки злоумышленника на пользователей информационной системы, представленных в виде графа социальных связей // Информатизация и связь. – 2015. – № 2. – С. 69–75.

17. Модель профиля компетенций злоумышленника в задаче анализа защищённости персонала информационных систем от социоинженерных атак / М.В. Абрамов, А.А. Азаров, Т.В. Тулупьева, А.Л. Тулупьев // Информационно-управляющие системы. – 2016. – №. 4 (83). – С. 77–84.

18. Approaches to development of models for text analysis of information in social network profiles in order to evaluate user’s vulnerabilities profile / G.I. Bagretsov, N.A. Shindarev, M.V. Abramov, T.V. Tulupyeva // Soft Computing and Measurements (SCM) : 2017 XX IEEE International Conference on. – IEEE, 2017. – pp. 93–95.

19. Вероятностные графические модели социально-значимого поведения индивида, учитывающие неполноту информации / А.В. Суворова, Т.В. Тулупьева, А.Л. Тулупьев, А.В. Сироткин, А.Е. Пащенко // Тр. СПИИРАН. – 2012. – Т. 3, №. 22. – С. 101–112.

20. Irani D., Webb S., Kang L., Calton P. Large online social footprints–an emerging threat // Computational Science and Engineering, 2009 : CSE'09. International Conference on. – IEEE, 2009. – Т. 3. – pp. 271–276.

21. Социально-психологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социоинженерных атак / Т.В. Тулупьева, А.Л. Тулупьев, А.Е. Пащенко, А.А. Азаров, М.В. Степашкин // Тр. СПИИРАН. – 2010. – Т. 1, № 12. – С. 200–214.

22. Абрамов М.В., Азаров А.А., Фильченков А.А. Распространение социоинженерной атаки злоумышленника на пользователей информационной системы, представленных в виде графа социальных связей // Международная конференция по мягким вычислениям и измерениям / Санкт-Петербургский государственный электротехнический университет ЛЭТИ им. В.И. Ульянова (Ленина). – 2015. – Т. 1. – С. 329–331.

23. Социальные сети в России: исследование Mail. Ru Group. – URL: https://corp.imgsmail.ru/media/files/issledovanie-auditorij-sotcialnykh-setej.pdf.

24. Studying user footprints in different online social networks / A. Malhotra, L. Totti, Jr W. Meira, P. Kumaraguru, V. Almeida // Advances in Social Networks Analysis and Mining (ASONAM) : 2012 IEEE/ACM International Conference on. – IEEE, 2012. – pp. 1065–1070.

25. Бартунов С., Коршунов А. Идентификация пользователей социальных сетей в Интернет на основе социальных связей // Тр. конф. по анализу изображений сетей и текстов (АИСТ). – 2012. – С. 5–22.

REFERENCES

1. *2012 Cost of Cyber Crime Study: United States, Ponemon Institute,* October 2012, p. 30. Available at: http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_ Study_FINAL6%20.pdf.

2. *2013 Cost of Cyber Crime Study: United States, Ponemon Institute,* October 2013, p. 30. Available at: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_1345 5.pdf.

3. *2014 Cost of Cyber Crime Study: United States, Ponemon Institute,* October 2014, p. 30. Available at: http://resources.idgenterprise.com/original/AST-0130677_2014_US_Cost_of_ Cyber_Crime_Study_FINAL_2.pdf.

4. *2015 Cost of Cyber Crime Study: Global, Ponemon Institute,* October 2015, p. 30. Available at: https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf.

5. *2016 Cost of Cyber Crime Study & the Risk of Business Innovation: Global, Ponemon Institute,* October 2016, p. 37. Available at: http://www.ponemon.org/local/upload/file/2016 %20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

6. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. *Kaspersky Lab,*

2017. Available at: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (accessed: 06.10.2017).

7. Antonyuk E.M., Varshavsky I.E., Antonyuk P.E. Adaptive Systems of Automatic Control with Prioritized Channels. *Soft Computing and Measurements (SCM). 2017 XX IEEE International Conference on.* IEEE, 2017, pp. 539–540.

8. Desnitsky V.A., Kotenko I.V. Modeling and Analysis of Security Incidents for Mobile Communication Mesh Zigbee-Based Network. *Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on.* IEEE, 2017, pp. 500–502.

9. Kotenko I., Chechulin A., Branitskiy A. Generation of Source Data for Experiments with Network Attack Detection Software. *Journal of Physics: Conference Series.* IOP Publishing, 2017, vol. 820, no. 1, p. 012033.

10. Azarov A.A., Tulupieva T.V., Suvorova A.V., Tulupiev A.L., Abramov M.V., Iusupov R.M. *Sotsioinzhenernye ataki: problemy analiza* [Social Engineering Attacks: Problems of Analysis]. St. Petersburg, Nauka Publ., 2016. 352 p.

11. Vkontakte vyplatila polzovateliam bolee $70 tysiach za poisk uiazvimostei [Vkonakte payed users more than $70 thousand for searching holes]. *Novosti Mail.ru* [Mail.ru News]. Available at: https://news.mail.ru/economics/25792158/ (accessed 12.12.2017).

12. Kak zashchitit vnutrenniuiu set i sotrudnikov kompanii ot atak, osnovannykh na ispolzovanii sotsiotekhniki [How to Protect an Internal Network and Employees of a Company against attacks based on the Application of Social Engineering]. *Microsoft,* 2007. Available at: https://technet.microsoft.com/ru-ru/library/cc875841.aspx (accessed 12.12.2017).

13. Anoshin I. Kartochnye slabosti. Kak ne stat zhertvoi vysokotekhnologichnykh mo-shennikov [Card Weakness. How to Prevent from Becoming Victims of High Technology Cheaters]. *RBK. Gazeta no. 164* [RBK. Newspaper no. 164]. Available at: http://www.rbc.ru/newspaper/2017/09/29/59ca447 b9a79474aa6f65673.

14. Mitnik K.D., Saymon V.L. *Iskusstvo obmana* [Art of Deception]. Moscow, IT Com-pany Publ., 2004. 416 p.

15. Shindarev N., G. Bagretsov, M. Abramov, T. Tulupyeva, A. Suvorova. Approach to Identifying of Employees Profiles in Websites of Social Networks Aimed to Analyze Social Engineering Vulnerabilities. *Advances in Intelligent Systems and Computing. Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'17).* 2017, vol. 1, pp. 441–447.

16. Abramov M.V., Azarov A.A. Analiz rasprostraneniia imitirovannoi sotsioinzhenernoi ataki zloumyshlennika na polzovatelei informatsionnoi sistemy, predstavlennykh v vide grafa sotsialnykh sviazei [Analysis of the Propagation Simulated Socio-Engineering Malicious Attacks on Users of Information Systems Presented as a Graph of Social Ties]. *Informatizatsiia i sviaz* [Informatization and Communication], 2015, no. 2, pp. 69–75.

17. Abramov M.V., Azarov A.A., Tulupieva T.V., Tulupiev A.L. Model profilia kompetentsii zloumyshlennika v zadache analiza zashchishchennosti personala informatsionnykh sistem ot sotsioinzhenernykh atak [Model of Malefactor Competencies Profile for Analyzing Information System Personnel Security from Social Engineering Attacks]. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 4 (83), pp. 77–84.

18. Bagretsov G.I., Shindarev N.A., Abramov M.V., Tulupyeva T.V. Approaches to Development of Models for Text Analysis of Information in Social Network Profiles in Order to Evaluate User's Vulnerabilities Profile. *Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on.* IEEE, 2017, pp. 93–95.

19. Suvorova A.V., Tulupyeva T.V., Tulupyev A.L., Sirotkin A.V., Pashchenko A.E. Veroiatnostnye graficheskie modeli sotsialno-znachimogo povedeniia individa, uchityvaiushchie nepolnotu informatsii [Probabilistic Graphical Models of Individual Socially Significant Behavior on the Base of Incomplete Data]. *Tr. SPIIRAN* [SPIIRAS Proceedings], 2012, vol. 3, no. 22, pp. 101–112.

20. Irani D., Webb S., Kang L., Calton P. Large Online Social Footprints–an Emerging Threat. *Computational Science and Engineering, 2009. CSE'09. International Conference on.* IEEE, 2009, vol. 3, pp. 271–276.

21. Tulupyeva T.V., Tulupyev A.L., Pashchenko A.E., Azarov A.A., Stepashkin M.V. Sotsialno-psikhologicheskie faktory, vliiaiushchie na stepen uiazvimosti polzovatelei avtomatizirovannykh informatsionnykh sistem s tochki zreniia sotsioinzhenernykh atak [Social Psychological Factors that Influence the Information System Users Vulnerability Degree in Regard of Social Engineering Attacks]. *Tr. SPIIRAN* [SPIIRAS Proceedings], 2010, vol. 1, no. 12, pp. 200–214.

22. Abramov M.V., Azarov A.A., Filchenkov A.A. Rasprostranenie sotsioinzhenernoi ataki zloumyshlennika na polzovatelei informatsionnoi sistemy, predstavlennykh v vide grafa sotsialnykh sviazei [Spread of Social Engineering Attacks on Users of Information System Presented as a Graph of Social Ties]. *Mezhdunarodnaia konferentsiia po miagkim vychisleniiam i izmereniiam* [International Conference on Soft Computing and Measurements]. Federalnoe gosudarstvennoe avtonomnoe obrazovatelnoe uchrezhdenie vysshego obrazovaniia Sankt-Peterburgskii gosudarstvennyi elektrotekhnicheskii universitet LETI im. V.I. Ulyanova (Lenina) Publ., 2015, vol. 1, pp. 329–331.

23. *Sotsialnye seti v Rossii: issledovanie Mail.Ru Group* [Social Media Platforms in Russia: Mail.Ru Group Research]. Available at: https://corp.imgsmail.ru/media/files/issledovanie-auditorij-sotcialnykh-setej.pdf.

24. Malhotra A., L. Totti, Jr W. Meira, P. Kumaraguru, V. Almeida. Studying User Footprints in Different Online Social Networks. *Advances in Social Networks Analysis and Mining (ASONAM). 2012 IEEE/ACM International Conference on*. IEEE, 2012, pp. 1065–1070.

25. Bartunov S., Korshunov A. Identifikatsiia polzovatelei sotsialnykh setei v Internet na osnove sotsialnykh sviazei [User Identification of Social Media Platforms in Internet on the Base of Social Ties]. *Tr. konf. po analizu izobrazhenii setei i tekstov (AIST)* [Proceedings of the Conference on Analysis of Network and Text Representation]. 2012, pp. 5–22.