УДК 004.8

Подход наибольшего правдоподобия к задаче выявления траекторий социоинженерных атак и скомпрометированных пользователей информационных систем

Хлобыстова А. О., Абрамов М. В., Тулупьев А. Л.

Постановка задачи: *сегодня одной из важных проблем информационной безопасности для организаций является рост числа успешных социоинженерных атак. Существенной особенностью таких атак является сложность расследования инцидентов, связанных с ними. В настоящее время уже существуют методы расследования инцидентов информационной безопасности, произошедших за счет использования злоумышленником программно-технических уязвимостей, однако аналогичных широко используемых инструментов в случае инцидентов, связанных с социоинженерными атаками, не имеется.* ***Целью работы*** *является усовершенствование инструментария расследования инцидентов информационной безопасности за счет разработки подходов наибольшего правдоподобия, направленных на выявление сценариев (траекторий) развития социоинженерных атак и скомпрометированных пользователей информационных систем. В качестве* ***используемых методов*** *в статье выступают вероятностный подход к оценке степени уязвимости пользователей к социоинженерным атакам, графовая модель представления информационной системы организации, в которой отражены профили пользователей и взаимосвязи между ними, а также доступные им критические документы.* ***Новизна*** *работы заключается в том, что ранее расследование инцидентов информационной безопасности основывалось только на технических характеристиках и не учитывало подверженность персонала социоинженерному воздействию. В настоящей статье предлагается подход, основывающийся на оценках вероятности успеха одноходовых и многоходовых социоинженерных атак, опирающихся в том числе на профиль уязвимостей пользователя.* ***Результатом*** *работы является подход, позволяющий осуществлять первичное расследование инцидентов информационной безопасности, связанных с реализацией социоинженерных атак, за счет разработки метода наибольшего правдоподобия, направленного на выявление траекторий социоинженерных атак и скомпрометированных пользователей информационных систем.* ***Практическая значимость*** *полученных результатов заключается в формировании инструмента для лиц, принимающих решения, дающем возможность сократить пространство поиска при расследовании инцидентов, связанных с успешной реализацией социоинженерной атаки; минимизировать время, необходимое для расследования преступления; определить основу для последующей разработки рекомендательных систем, способствующих понижению рисков реализации социоинженерных атак.*

Ключевые слова: *социоинженерные атаки, информационно-психологическое воздействие, бэктрекинг инцидентов, расследование атак, траектории распространения, информационная безопасность, защита пользователя, уязвимость пользователя, социальные сети, социальный граф.*

Библиографическая ссылка на статью:
Хлобыстова А. О., Абрамов М. В., Тулупьев А. Л. Подходы наибольшего правдоподобия к задаче выявления траекторий социоинженерных атак и скомпрометированных пользователей информационных систем // Системы управления, связи и безопасности. 2019. № 3. С. 202-219. DOI: 10.24411/2410-9916-2019-10310.

Reference for citation:
Khlobystova A. O., Abramov M. V., Tulupyev A. L. Maximum likelihood estimation methods of social engineering attack trajectories detection and information system compromised users revelation. *Systems of Control, Communication and Security*, 2019, no. 3, pp. 202-219. DOI: 10.24411/2410-9916-2019-10310 (in Russian).

Актуальность

Одной из важных проблем для организаций сегодня является рост числа киберпреступлений, совершаемых с применением методов социальной инженерии. Такие киберпреступления называются социоинженерными атаками. Под социоинженерными атаками в данной статье понимается набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности [1]. Так, по данным Сбербанка в 2019 году социоинженерные атаки вошли в тройку трендов в области киберпреступлений [2], а также стали самым распространённым видом кибермошеничества в 2018 году [3]. Кроме того, согласно данным TS Solution [4], в 95% случаях успешно реализованных атак в организации уже были внедрены решения для защиты от киберугроз. Как правило, такие решения направлены на минимизацию рисков реализации атак, эксплуатирующих только программно-технические уязвимости. По данным компании Verizon [5], проанализировавшей более 41 тысячи инцидентов нарушения информационной безопасности за 2018–2019 гг., руководители высшего звена, имеющие доступ к конфиденциальным данным, в 12 раз чаще становятся целью социоинженерных атак нежели рядовые сотрудники. Кроме того, отмечается, что 85% различных ошибок, ставящих под угрозу безопасность конфиденциальных данных организации, были вызваны непреднамеренными действиями сотрудников организации [5]. Актуальность проблемы социоинженерных атак также подтверждают и данные Центрального банка Российской Федерации [6], согласно которым за 2018 год объём несанкционированных операций по платёжным картам составил 1,38 млрд рублей, в 97% случаев были использованы методы социальной инженерии. Также важность повышения уровня защищённости от социоинженерных атак как частных лиц, так и сотрудников организаций подчеркивается многочисленными инцидентами, широко освещающимися в системах массовой информации [7-9]. Т.е. проблема защиты пользователей от социоинженерных атак чрезвычайно актуальна в настоящее время. Однако большая часть исследований в области информационной безопасности сегодня посвящена вопросам защиты информационных систем от программно-технических атак [11-14], тема защиты пользователей от социоинженерных атак исследована в меньшей степени.

Существуют исследования по проблеме анализа защищенности пользователей от социоинженерных атак [15-17], которые направлены на разработку комплекса программ для автоматизированного построения оценок защищенности пользователей. Тем не менее, не всегда удаётся избежать реализации социоинженерной атаки и организации сталкиваются с ситуациями, когда есть сведения лишь о том, что в отношении некоторых критичных ресурсов информационной системы нарушены свойства информационной безопасности. При этом зачастую неизвестна информация о том, каким образом была реализована атака, какие пользователи информационной системы оказались скомпрометированы, сколько и какие критичные документы были

успешно атакованы (т.е. в отношении нарушены свойства информационной безопасности) и т.п. Для ответов на эти вопросы обычно проводится расследование, правильно использованные результаты которого способствуют минимизации ущерба от атаки, сокращению рисков реализации новых социоинженерных атак. Чем оперативнее и точнее будет проведено данное расследование, тем выше будет его эффективность. Таким образом, актуальной видится задача разработки инструментов, помогающих в проведении подобных расследований, способствующих их оперативности и точности. Данная статья направлена на разработку подхода наибольшего правдоподобия в выявлении траекторий социоинженерных атак и скомпрометированных пользователей информационных систем, для упрощения проведения расследования произошедших социоинженерных атак.

Практическая значимость такого подхода заключается в потенциале его применения к инструментарию, направленному на обеспечение возможности оперативного получения комплексного представления о сценарии произошедшего инцидента. Эти инструменты позволят оперативно получать информацию и использовать её при принятии мер, редуцирующих риски новых инцидентов. Полученные результаты обладают научной новизной, задача в такой формулировке ставится впервые, подход к выявлению траекторий социоинженерных атак и скомпрометированных пользователей информационных систем ранее не предлагался.

Анализ известных работ в исследуемой предметной области

Исследования [10-14] фокусируются на расследовании киберинцидентов, в которых использовались исключительно программно-технические уязвимости информационных систем. Однако несмотря на техническую направленность работ, некоторые из представленных в них подходов могут быть применимы и к расследованию социоинженерных атак. Так, к примеру, исследование [12] основывается на онтологии цифровых криминалистических событий, которая может быть применима на начальном этапе проведения криминалистического анализа для восстановления событий атаки. А именно авторы предлагают автоматизировать процесс анализа низкоуровневых «цифровых искажений», выявляя артефакты, требующие дальнейшего изучения. Схожий подход применяется и в настоящем исследовании, однако основывается на информации о профилях защищённости пользователей и силах связей между ними.

В [20] отмечается разнообразие личных данных, которые могут быть получены из социальных сетей, а также перечисляются риски, связанные с нарушением конфиденциальности. К примеру, показано, что по информации о «лайках» пользователя можно предсказать его гендерную ориентацию, этническую принадлежность, религию, политическую направленность, некоторые характеристики личности, уровень IQ, склонность к употреблению наркотиков и др. Также приводится информация о том, что студенты, получившие высокие оценки по экстраверсионным характеристикам, принадлежали к большему количеству групп в Facebook, но у них было очень

мало друзей (причина: предпочитают мгновенный контакт с друзьями), а люди с высоким уровнем невротизма предпочитали делать пост на свою стену, а не публиковать свои фотографии. Такая информация может быть полезна при построении профиля уязвимостей пользователя, оценок вероятности успеха при распространении социоинженерной атаки на социальном графе.

Авторы [22] сосредотачиваются на исследовании факторов (экзогенных (внутренних: структура сети) и эндогенных (внешних: активность менеджера сообщества, инвестиции компании в цифровой маркетинг и др.), влияющих на взаимодействие пользователей на основе социальной сети Facebook. Для целей текущего исследования наиболее интересны экзогенные факторы, а именно динамика социального взаимодействия в социальном графе, основывающаяся на свойствах структуры сети. Согласно [22] верна гипотеза о существовании прямой связи между плотностью социального графа и взаимодействием пользователей в социальной сети, а также о прямой связи между кластеризацией социального графа (выделением более плотных участков сети) и взаимодействием пользователей в социальной сети. Полученная гипотеза находит своё применение при построении оценок распространения многоходовых атак злоумышленника.

Социоинженерные атаки также могут быть рассмотрены как вид информационно-психологических воздействий, оказывающих влияние на восприятие человеком реальной действительности, в частности на его поведенческие функции [23]. Так при построении профиля уязвимостей пользователя и профиля компетенции злоумышленника может быть использована классификация видов, средств, способов и тактических приемов информационного воздействия, подробно представленная в [24]. Также одно из направлений развития используемых в подходе моделей видится в рассмотрении информационно-психологического оружия как атакующего воздействия [25], в том числе распространение информации в социальных сетях [26].

Вопросы построения формализованных моделей оценки изменения сознания людей под влиянием внешних воздействий были рассмотрены в [27]. Полученные авторами модели могут быть применимы в дальнейших исследованиях при моделировании социоинженерных атак с учётом ограниченности ресурса злоумышленника. В задаче моделирования социоинженерного воздействия также находит своё применение и результаты, полученные в [28], автором которой поднимается проблема выявления предрасположенностей пользователей к информационному воздействию в зависимости от места и роли субъекта в социальной структуре. Также при построении рекомендательной системы, направленной на предотвращение неправомерных действий пользователей информационных систем, может быть полезно исследование [29].

Заделом для настоящего исследования послужили работы [1, 18-19, 30-31]. В частности, в [1] была представлена модель «критичные документы – информационная система – персонал – злоумышленник», предложены методы автоматизированного сбора и обработки сведений из социальных сетей для

оценки параметров модели пользователя и межпользовательских связей, дано определение многоходовых социоинженерных атак и представлены подходы к оценке вероятности сценариев реализации атак. В [30] был описан подход к оценке критичности траекторий распространения многоходовых социоинженерных атак, однако были рассмотрены не все возможные конфигурации прав распределения доступа к документам разного уровня критичности, а также не был затронут вопрос расследования инцидентов.

Постановка задачи

Несмотря на существующие наработки в области защиты пользователей от социоинженерных атак, нередко организации сталкиваются с ситуацией, когда атака уже произошла, но доступны только сведения о том, что некоторые критичные ресурсы информационной системы были успешно атакованы. В таком случае специалистам компании в области информационной безопасности приходится производить расследование произошедшего инцидента. При этом процесс расследования социоинженерной атаки весьма трудоёмкий и включает в себя комплексный анализ большого числа составляющих информационной системы [13]. Поэтому возникает задача разработки подходов к автоматизации или частичной автоматизации данного процесса. Целью настоящей статьи является усовершенствование инструментария расследования инцидентов информационной безопасности за счет разработки подходов наибольшего правдоподобия, направленных на выявление сценариев развития социоинженерных атак и скомпрометированных пользователей информационных систем, основывающихся на анализе социального графа сотрудников организации.

Под социальным графом сотрудников организации будем понимать ориентированный взвешенный граф, вершины которого – это пользователи информационной системы [1], а рёбра – взаимосвязи между ними, каждому ребру сопоставлена оценка вероятности успеха прохождения социоинженерной атаки от одного пользователя к другому. Предполагается, что оценка вероятности успеха прохождения социоинженерной атаки между пользователями зависит от характера их взаимоотношений, интенсивности взаимодействия, информацию о которых можно извлечь из социальных сетей [15]. Предположим, что дан социальный граф сотрудников некоторой организации $G=(U,E)$, где $U=\{U_i\}_{i=1}^{n}$ – множество вершин (пользователей), $E=\left\{(U_i,U_j,p_{i,j})\right\}_{1\le i,j\le n,i\ne j}$ – множество упорядоченных троек с заданной оценкой вероятности распространения атаки от пользователя U_i к пользователю U_j. Также дана информация о критичных документах, имеющихся в информационной системе: $D=\{D_j\}_{1\le j\le m}$ – множество критичных документов. $A=\left\{(U_i,D_j)\right\}_{1\le i\le n,1\le j\le m}$ – множество пар, соответствующее пользователям информационной системы и документам, к которым они имеют

доступ. Таким образом, рассматриваем объект $G' = (U, E, D, A)$. Задача заключается в восстановлении сценария развития социоинженерной атаки на основе информации о том, что документ (D_i) был успешно атакован. Под сценарием развития социоинженерной атаки на социальном графе сотрудников организации понимается множество наиболее вероятных путей распространения атаки – множество траекторий атаки.

Подходы к расследованию

Социоинженерные атаки могут быть разделены на прямые (одноходовые) и многоходовые [1]. Одноходовые атаки характеризуются таргетированным воздействием на выбранного пользователя информационной системы. Атака, в которой задействован более чем один сотрудник, а успешно атакованные пользователи непосредственно участвуют во взломе последующих жертв называется многоходовой социоинженерной атакой [1]. Далее будут рассмотрены подходы к выявлению сценариев развития обоих типов атак: одноходовых (прямых) и многоходовых.

Прямая социоинженерная атака

Предположим, что документ D_i был успешно атакован при социоинженерном воздействии. Найдём множество всех $\{U_j : (U_j, D_i) \in A\}$, то есть пользователей, у которых есть доступ к атакованному документу. Согласно [1] модель пользователя информационной системы (узлов социального графа) содержит, в том числе и информацию об оценке вероятности успеха социоинженерной атаки на него (p_j). Отсечём пользователей, с оценками успеха прямой атаки на них ниже определённого уровня. Для этого ведём пороговое значение thr_U, соответствующее низкому уровню оценки успеха прямой социоинженерной атаки, при достижении которого $(p_j < t_U)$ пользователь не будет учитываться в дальнейшем. На основе этой информации рассмотрим множество $S^{(1)}$, которое содержит всех найденных пользователей $\{U_j : (U_j, D_i) \in A\}$, оценка вероятности успеха социоинженерной атаки на которых выше порогового значения $(p_j > t_U)$. Упорядочим это множество по убыванию значения оценки вероятности успеха социоинженерной атаки. Пусть k будет индексом, соответствующим порядку элемента в упорядоченном множестве $\{U_j^k : (U_j^k, D_i) \in A\}$, для каждого U_j^k в котором будет верно неравенство: $(p_j^k \geq \mathrm{p}_l^{k+1})$. Таким образом, множество $S^{(1)} = \{U_j^k : ((U_j^k, D_i) \in A) \wedge (p_j^k \geq \mathrm{p}_l^{k+1}, j \neq l) \wedge (p_j^k > t_{\mathrm{U}})\}$. На данном этапе множество $S^{(1)}$ будет содержать всех пользователей, которые могли быть подвержены прямой социоинженерной атаке. Таким образом, имеем первое предположение со списком пользователей информационной системы, которые, потенциально, могли быть успешно атакованы. Кроме того, имеем список

критичных документов, к которым был доступ у пользователей из вышеупомянутого списка. Такие документы также потенциально были успешно атакованы.

Многоходовая социоинженерная атака

Однако злоумышленник мог успешно атаковать не одного пользователя, а цепочку, произвести многоходовую социоинженерную атаку. По построенному множеству $S^{(1)}$, которое содержит потенциально причастных к социоинженерной атаке сотрудников, построим множество соответствующее возможным многоходовым атакам. Для отсечения траекторий развития социоинженерной атаки с низкими оценками вероятности успеха их реализации введём пороговое значение t_E. То есть если оценка вероятности прохождения злоумышленником по данной траектории будет ниже порогового значения $\left(p < t_{\text{E}}\right)$, то в дальнейшем такую траекторию рассматривать не будем. Для всех пользователей $U_j \in S^{(1)}$ найдём такие траектории $\left\{U_l : \left(\left(U_l, U_j, p_{l,j}\right) \in E\right) \wedge \left(p_{l,j} > t_E\right)\right\}$, где $E = \left\{(U_l, U_j, p_{i,j})\right\}_{1 \le l,\, j \le n, l \ne j}$ – множество упорядоченных троек с заданной оценкой вероятности распространения атаки от пользователя U_l к пользователю U_j – $p_{l,j}$, а t_E – пороговое значение, соответствующее низкой оценке вероятности успеха реализации траектории атаки. В предположении, что события независимы, вероятность успеха многоходовой социоинженерной атаки может быть рассчитана по следующей формуле: $p_T = p_i \cdot \prod_{l=i}^{j-1} p_{l,l+1}$, где $j > 1$, $T = \left(U_i, E_i, ..., E_{j-1}, U_j\right)$, p_i – оценка вероятности успеха социоинженерной атаки на пользователя i, а $p_{l,l+1}$ – оценка вероятности распространения атаки от пользователя U_l к пользователю U_{l+1}, а $\left|T\right|$ – число вершин, входящих в траекторию [30]. Не умаляя общности рассуждений, будем считать, что мощность траектории, т.е. число вершин, входящих в траекторию, $\left|T\right| \ge 1$ и в случае, если $\left|T\right| = 1$, то $p_T = p_i$. Под $\left|T\right|$ понимается число вершин, входящих в траекторию. В случае, если число вершин равно единице, то мы имеем дело с одноходовой атакой.

Дополнительно отметим, что при расчёте оценки вероятности успеха многоходовой социоинженерной атаки считается, что события (эпизоды, характеризующие интенсивность взаимодействия сотрудников в компании, или поражение одного пользователя через другого) являются независимыми. Т.е. успех атаки пользователя 3 через пользователя 2 не зависит от успеха атаки пользователя 2 через пользователя 1. Если при дальнейшем исследовании окажется, что рассматриваемые события зависимы, то для расчёта оценок необходимо будет искать способы описать ситуацию так, что можно было бы рассуждать о независимых событиях. Одним из инструментов для этого может

стать аппарат алгебраических байесовских сетей, указанный подход к релаксации требования независимости рассматривается более детально в [30]. Тем не менее погрешности при зависимых событиях могут оказаться настолько незначительными, что будут покрываться текущими оценками.

Пусть множество $S^{(2)}$ будет соответствовать многоходовой социоинженерной атаке, в которой был успешно атакован документ D_i и были задействованы два пользователя:

$$S^{(2)} = \left\{ T^k = (U_l, E_{l,j}, U_j) : \left(U_j \in S^{(1)}\right) \wedge \left(p_{T^k} > t_E\right) \wedge \left(p_{T^k} \geq p_{T^{k+1}}\right) \right\},$$

где T^k – k-ая траектория реализации социоинженерной атаки, при которой первым скомпрометированным пользователем (точкой вхождения в информационную систему) был User_l, доступ к критичному документу был получен через пользователя User_j, а вероятность реализации данной траектории p_{T^k} не ниже порогового значения t_E (в данном случае индекс k указывает на порядок траектории в упорядоченном по вероятности успеха её реализации множестве). Аналогичным образом построим множество $S^{(m)} = \left\{ T^k = (U_{l_1}, E_{l_1,l_2}, ..., E_{l_{m-1},l_m}, U_{l_m}) : \right.$

$\left. \left(p_{T^k} > t_E\right) \wedge \left(p_{T^k} \geq p_{T^{k+1}}\right) \wedge \left(\left(U_{l_2}, E_{l_2,l_3}, ..., E_{l_{m-1},l_m}, U_{l_m}\right) \in S^{(m-1)}\right) \right\}$, соответствующее сценарию развития социоинженерной атаки, при котором было задействовано m пользователей и успешно атакован документ D_i. Построение множеств $S^{(m)}$ будет закончено в тот момент, когда последующее множество будет пустым $\left(S^{(m+1)} = \varnothing\right)$.

Пусть $S = \bigcup_{j=1}^{m} S^{(i)} = \left\{ T^k : \left(p_{T^k} \geq p_{T^{k+1}}\right) \right\}$, то есть множество S будет содержать все возможные сценарии развития социоинженерной атаки, упорядоченные по убыванию вероятности их реализации.

Полученное множество S может быть визуализировано в виде графа с градиентным выделением узлов, которые могли быть атакованы с наибольшей вероятностью. После чего само множество S и его графовое представление будет направлено специалистам отдела безопасности для дальнейшего расследования инцидента, включающего непосредственное взаимодействии с сотрудниками организации.

Практическое применение

Рассмотрим применение предложенных подходов на примере информационной системы, представленной на рис. 1.

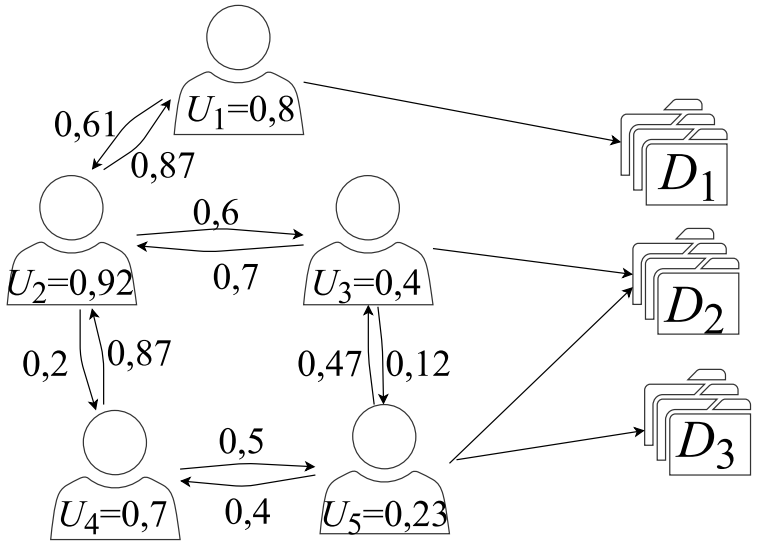

Рис. 1. Пример информационной системы

Пусть нам известно, что документ D_2 был успешно атакован злоумышленником-социоинженером. Тогда множество всех пользователей, у которых есть доступ к атакованному документу будет состоять из двух элементов: $\{U_3, U_5\}$. Положим $t_U = 0{,}1$. Проверим элементы множества на соответствие пороговому значению и упорядочим их по убыванию значения оценки вероятности успеха социоинженерной атаки. Тогда множество $S^{(1)} = \{U_3^1, U_5^2\}$ (выделено светло-серым цветом на рис. 2).

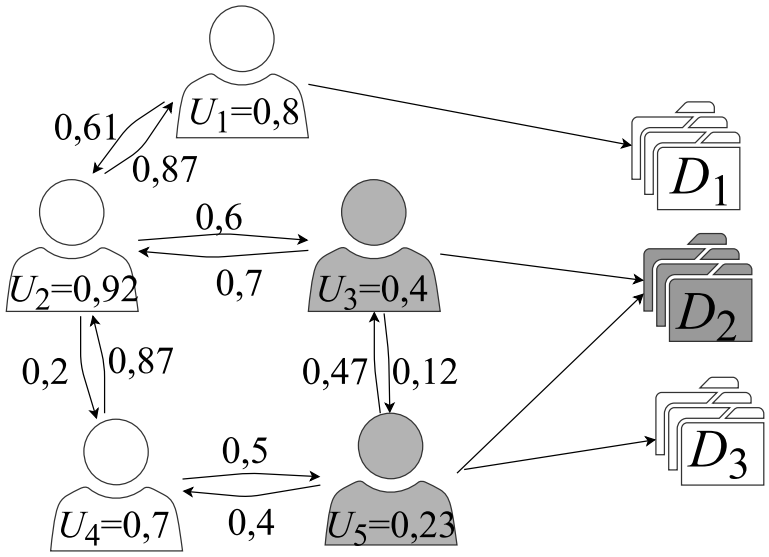

Рис. 2. Нахождение сценариев развития одноходовой социоинженерной атаки

Предположим, что могла быть совершена многоходовая социоинженерная атака. Пусть $t_E = 0{,}1$. Рассмотрим, как будет осуществлен поиск траекторий, в которых задействован пользователь $U_3 \in S^{(1)}$, а число вершин входящих в траекторию равно 2 $(|T| = 2)$. Согласно рис. 1 пользователь

U_3 с вероятностью $p_{2,3}=0,6$ мог быть атакован через U_2 и $p_{5,3}=0,47$ через U_5. Тогда вероятность реализации сценария $T=\left(U_2,E_{2,3},U_3\right)$ будет равна $p_T=p_2p_{2,3}=0,92\cdot0,6=0,552,$ а сценария $T=\left(U_5,E_{5,3},U_3\right)$ – $p_T=p_5p_{5,3}=0,23\cdot0,47=0,1081.$ Аналогично посчитаны сценарии развития атаки, в которых задействован пользователь U_5. После их упорядочивания множество

$$S^{(2)}=\left\{T^1=(U_2,E_{2,3},U_3),T^2=(U_4,E_{4,5},U_5),T^3=(U_5,E_{5,3},U_3)\right\}.$$

Отметим, что траектория $(U_3,E_{3,5},U_5)$ была снята с рассмотрения, так как вероятность их реализации составляет $0,048,$ что меньше установленного порогового значения.

После нахождения всех траекторий, расчёта вероятности их реализации и упорядочивания получено множество $S=\left\{(U_2,E_{2,3},U_3),U_3,(U_4,E_{4,5},U_5),\right.$ $(U_1,E_{1,2},U_2,E_{2,3},U_3),\ U_5,(U_4,E_{4,5},U_5,E_{5,3},U_3),\ \left.(U_5,E_{5,3},U_3)\right\}.$

Выводы

Таким образом, в работе был представлен подход к расследованию киберинцидента, совершенного с применением методов социальной инженерии. Данный подход основывается на сведениях об успешно атакованных критичных ресурсах информационной системы и социальном графе сотрудников организации, который включает в себя профили уязвимостей пользователей организации, информацию о взаимосвязях между ними и доступным им критичным документам.

Новизна работы заключается в ряде аспектов, которые связаны с одной стороны с учетом исключительно программно-технических компонентов, способствующих обеспечению информационной безопасности, с другой стороны, с отсутствием цифровых двойников, устоявшихся формализаций проблемно-ориентированных, информационных, социотехнических систем, основанных на анализе доступных сведений о них, обработке и представлении данных и знаний с неопределенностью. Данный подход может служить основой для проектирования автоматизированной системы, которая по заданному критическому документу, строит граф сотрудников и связей между ними с выделением узлов, имеющих наибольшую вероятность причастности к произошедшей социоинженерной атаки.

Практическая значимость полученных результатов заключается в формировании инструмента для лиц, принимающих решения, дающем возможность сократить пространство поиска при расследовании инцидентов, связанных с успешной реализацией социоинженерной атаки; минимизировать время, необходимое для расследования преступления; определить основу для последующей разработки рекомендательных систем, способствующих понижению рисков реализации социоинженерных атак.

В качестве дальнейших исследований предлагается рассмотреть возможность применения теории коэффициентов уверенности и доверия при составлении профиля уязвимостей пользователя.

Работа выполнена в рамках проекта по государственному заданию СПИИРАН № 0073-2019-0003 и при финансовой поддержке РФФИ (гранты №18-01-00626, № 18-37-00323).

Литература

1. Абрамов М. В., Тулупьева Т. В., Тулупьев А. Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с.

2. Сбербанк назвал три тренда в области киберпреступлений // РИА Новости [Электронный ресурс]. 19.05.2019. – URL: https://ria.ru/20190427/1553112124.html (дата обращения 19.05.2019).

3. Сбербанк назвал самый распространенный вид кибермошенничества // Новости Рамблер [Электронный ресурс]. 19.05.2019. – URL: https://news.rambler.ru/other/41347408-sberbank-nazval-samyy-rasprostranennyy-vid-kibermoshennichestva/ (дата обращения 19.05.2019).

4. Опасности цифровизации или цифровизация в опасности // Digital Forum РБК [Электронный ресурс]. 19.05.2019. – URL: https://spb.plus.rbc.ru/news/5cb448c57a8aa90a3814c68e (дата обращения 19.05.2019).

5. 2019 Data Breach Investigations Report // Verizon [Электронный ресурс]. 22.05.2019. – URL: https://enterprise.verizon.com/resources/reports/dbir/ (дата обращения 22.05.2019).

6. ЦБ заметил рост объема несанкционированных операций по картам // РБК [Электронный ресурс]. 21.05.2019. – URL: https://www.rbc.ru/finances/19/02/2019/5c6bd7379a7947620167c4b0#ws (дата обращения 21.05.2019).

7. Почти 865 000 рублей похищено с банковских счетов ижевчанина под предлогом предотвращения незаконной транзакции // МВД [Электронный ресурс]. 21.05.2019. – URL: https://18.xn--b1aew.xn--p1ai/news/item/16913340 (дата обращения 21.05.2019).

8. State Agencies, Department of Human Services Offices, Being Hit Hard by Phishing Scams // Minnesota Department of Human Services [Электронный ресурс]. 22.05.2019. – URL: http://stmedia.startribune.com/documents/2019-04-09_DHS_Data_Breach_Letter_to_Legislators.pdf (дата обращения 22.05.2019).

9. Oregon Department of Human Services Notifies Public of Data Breach // Oregon Department of Human Services [Электронный ресурс]. 22.05.2019. – URL: https://www.oregon.gov/DHS/DHSNEWS/NewsReleases/Data-Breech-News%20Release-2019-03-21.pdf (дата обращения 22.05.2019).

10. Ломако А. Г., Овчаров В. А., Петренко С. А. Метод расследования инцидентов безопасности на основе профилей поведения сетевых объектов // Дистанционные образовательные технологии. 2018. – С. 366–373.

11. Asim M., Amjad M. F., Iqbal W., Afzal H., Abbas H., Zhang Y. AndroKit: A toolkit for forensics analysis of web browsers on android platform // Future Generation Computer Systems. 2019. Vol. 94. P. 781–794. doi: 10.1016/j.future.2018.08.020

12. Turnbull B., Randhawa S. Automated event and social network extraction from digital evidence sources with ontological mapping // Digital Investigation. 2015. Vol. 13. P. 94–106. doi: 10.1016/j.diin.2015.04.004

13. Forensic investigation of a Social Engineering attack, from real life // Erdal Ozkaya [Электронный ресурс]. 23.07.2019. – URL: https://www.erdalozkaya.com/forensic-investigation-of-a-social-engineering-attack-from-real-life/ (дата обращения 23.07.2019).

14. Yaqoob I., Hashem I. A. T., Ahmed A., Kazmi S. A., Hong C. S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges // Future Generation Computer Systems. 2019. Vol. 92. P. 265–275. doi: 10.1016/j.future.2018.09.058

15. Li H., Luo X. R., Zhang J., Sarathy R. Self-control, organizational context, and rational choice in Internet abuses at work. Information & Management. 2018. Vol. 55. No. 3. P. 358–367. doi: 10.1016/j.im.2017.09.002

16. Aldawood H., Skinner G. Educating and raising awareness on cyber security social engineering: A literature review // 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). – IEEE, 2018. – P. 62–68. doi: 10.1109/TALE.2018.8615162

17. Kaushalya S., Randeniya R., Liyanage A. D. S. An Overview of Social Engineering in the Context of Information Security // 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS). – IEEE, 2018. – P. 1–6. doi: 10.1109/ICETAS.2018.8629126

18. Shindarev N., Bagretsov G., Abramov M., Tulupyeva T., Suvorova A. Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities // International Conference on Intelligent Information Technologies for Industry – Springer, Cham. 2018. Vol. 679. P. 441–447. doi: 10.1007/978-3-319-68321-8_45

19. Suleimanov A., Abramov M., Tulupyev A. Modelling of the social engineering attacks based on social graph of employees communications analysis // 2018 IEEE Industrial Cyber-Physical Systems (ICPS). – IEEE, 2018. P. 801–805. doi: 10.1109/ICPHYS.2018.8390809

20. Mansour R. F. Understanding how big data leads to social networking vulnerability // Computers in Human Behavior. 2016. Vol. 57. P. 348–351. doi: 10.1016/j.chb.2015.12.055

21. Curtis S. R., Rajivan P., Jones D. N., Gonzalez C. Phishing attempts among the dark triad: Patterns of attack and vulnerability // Computers in Human Behavior. 2018. Vol. 87. P. 174–182. doi: 10.1016/j.chb.2018.05.037

22. Maiz A., Arranz N., Fdez. de Arroyabe J. C. Factors affecting social interaction on social network sites: the Facebook case // Journal of Enterprise Information Management. 2016. Vol. 29. No. 5. P. 630–649. doi:10.1108/JEIM-10-2014-0105

23. Баришполец В. А. Информационно-психологическая безопасность: основные положения // Информационные технологии. 2003. Т. 3. № 2. С. 69–104.

24. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография – СПб.: Наукоемкие технологии. 2018. – 122 с.

25. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография – СПб.: Наукоемкие технологии. 2017. – 546 с.

26. Ажмухамедов И. М., Мачуева Д. А., Жолобов Д. А. Моделирование процесса распространения информации в социальных сетях // Фундаментальные исследования. 2017. № 5. С. 9–14.

27. Бухарин С. Н., Малков С. Ю. К вопросу о математическом моделировании информационных взаимодействий // Информационные войны. 2010. Т. 2. № 14. С. 14–20.

28. Расторгуев С. П. О проявлении скрытых в структуре системы предрасположенностей // Информационные войны. 2017. № 1. С. 92–97.

29. Новиков В. А., Демихов Е. Н. Подход к обоснованию управленческих решений на основе априорной истинности информации // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 5. С. 75–80.

30. Khlobystova A., Abramov M., Tulupyev A. An Approach to Estimating of Criticality of Social Engineering Attacks Traces // International Conference on Information Technologies – Springer, Cham, 2019. Vol. 199. P. 446–456. doi: 10.1007/978-3-030-12072-6_36

31. Хлобыстова А. О., Абрамов М. В., Тулупьев А. Л., Золотин А. А. Поиск кратчайшей траектории социоинженерной атаки между парой пользователей в графе с вероятностями переходов // Информационно-управляющие системы. 2018. № 6. С. 74–81. doi: 10.31799/1684-8853-2018-6-74-81

References

1. Abramov M. V., Tulupyeva T. V., Tulupyev A. L. Socioinjenernye ataki: socialnye seti i ocenki zashchishchennosti polzovatelei [Social Engineering Attacks: social networks and user security estimates]. Saint-Petersburg, State University of Aerospace Instrumentation, 2018. 266 p. (in Russian).

2. Sberbank nazval tri trenda v oblasti kiberprestuplenii [Sberbank lists the major trends in cybercrime]. *RIA News*, 19 May 2019. Available at: https://ria.ru/20190427/1553112124.html (accessed 19 May 2019) (in Russia).

3. Sberbank nazval samii rasprostranennii vid kibermoshennichestva [Sberbank called the most common form of cyber fraud]. *Rambler News*, 19 May 2019. Available at: https://news.rambler.ru/other/41347408-sberbank-nazval-samyy-rasprostranennyy-vid-kibermoshennichestva/ (accessed 19 May 2019) (in Russia).

4. Opasnosti cifrovizacii ili cifrovizaciya v opasnosti [Dangers of digitization or digitalization at risk]. *Digital Forum RBC*, 19 May 2019. Available at:

https://spb.plus.rbc.ru/news/5cb448c57a8aa90a3814c68e (accessed 19 May 2019) (in Russia).

5. 2019 Data Breach Investigations Report. *Verizon*, 22 May 2019. Available at: https://enterprise.verizon.com/resources/reports/dbir/ (accessed 22 May 2019).

6. CB zametil rost obema nesankcionirovannykh operacii po kartam [The Central Bank noted an increase in the volume of unauthorized card transactions]. *RBC*, 21 May 2019. Available at: https://www.rbc.ru/finances/19/02/2019/5c6bd7379a7947620167c4b0#ws (accessed 21 May 2019) (in Russia).

7. Pochti 865 000 rublei pokhishcheno s bankovskikh schetov ijevchanina pod predlogom predotvrashcheniya nezakonnoi tranzakcii [Almost 865,000 rubles were stolen from Izhevsk bank accounts under the pretext of preventing an illegal transaction]. *MIA of Russia*, 21 May 2019. Available at: https://18.xn--b1aew.xn--p1ai/news/item/16913340 (accessed 21 May 2019) (in Russia).

8. State Agencies, Department of Human Services Offices, Being Hit Hard by Phishing Scams. *Minnesota Department of Human Services*, 22 May 2019. Available at: http://stmedia.startribune.com/documents/2019-04-09_DHS_Data_Breach_Letter_to_Legislators.pdf (accessed 22 May 2019).

9. Oregon Department of Human Services Notifies Public of Data Breach. *Oregon Department of Human Services*, 22 May 2019. Available at: https://www.oregon.gov/DHS/DHSNEWS/NewsReleases/Data-Breech-News%20Release-2019-03-21.pdf (accessed 22 May 2019).

10. Lomako A. G., Ovcharov V. A., Petrenko S. A. Metod rassledovaniia intsidentov bezopasnosti na osnove profilei povedeniia setevykh ob''ektov [Method of investigation of security incidents based on the profiles of behavior of network objects]. *Distantsionnye obrazovatel'nye tekhnologii*, 2018, pp. 366–373 (in Russia).

11. Asim M., Amjad M. F., Iqbal W., Afzal H., Abbas H., Zhang Y. AndroKit: A toolkit for forensics analysis of web browsers on android platform. *Future Generation Computer Systems*, 2019, vol. 94, pp. 781–794. doi: 10.1016/j.future.2018.08.020

12. Turnbull B., Randhawa S. Automated event and social network extraction from digital evidence sources with ontological mapping. *Digital Investigation*, 2015, vol. 13, pp. 94–106. doi: 10.1016/j.diin.2015.04.004

13. Forensic investigation of a Social Engineering attack, from real life. *Erdal Ozkaya*, 23 July 2019. Available at: https://www.erdalozkaya.com/forensic-investigation-of-a-social-engineering-attack-from-real-life/ (accessed 23 July 2019).

14. Yaqoob I., Hashem I. A. T., Ahmed A., Kazmi S. A., Hong C. S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, 2019, vol. 92, pp. 265–275. doi: 10.1016/j.future.2018.09.058

15. Li H., Luo X. R., Zhang J., Sarathy R. Self-control, organizational context, and rational choice in Internet abuses at work. *Information & Management*, 2018, vol. 55, no. 3, pp. 358–367. doi: 10.1016/j.im.2017.09.002

16. Aldawood H., Skinner G. Educating and raising awareness on cyber security social engineering: A literature review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE).* – IEEE, Hong Kong, 2018, pp. 62–68. doi: 10.1109/TALE.2018.8615162

17. Kaushalya S., Randeniya R., Liyanage A. D. S. An Overview of Social Engineering in the Context of Information Security. *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS).* – IEEE, Bangkok, 2018, pp. 1–6. doi: 10.1109/ICETAS.2018.8629126

18. Shindarev N., Bagretsov G., Abramov M., Tulupyeva T., Suvorova A. Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities. *International Conference on Intelligent Information Technologies for Industry* – Springer, Cham, 2018, vol. 679, pp. 441–447. doi: 10.1007/978-3-319-68321-8_45

19. Suleimanov A., Abramov M., Tulupyev A. Modelling of the social engineering attacks based on social graph of employees communications analysis. *2018 IEEE Industrial Cyber-Physical Systems (ICPS).* – IEEE, 2018, pp. 801–805. doi: 10.1109/ICPHYS.2018.8390809

20. Mansour R. F. Understanding how big data leads to social networking vulnerability. *Computers in Human Behavior*, 2016, vol. 57, pp. 348–351. doi: 10.1016/j.chb.2015.12.055

21. Curtis S. R., Rajivan P., Jones D. N., Gonzalez C. Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior*, 2018, vol. 87, pp. 174–182. doi: 10.1016/j.chb.2018.05.037

22. Maiz A., Arranz N., Fdez. de Arroyabe J. C. Factors affecting social interaction on social network sites: the Facebook case. *Journal of Enterprise Information Management*, 2016, vol. 29, no. 5, pp. 630–649. doi:10.1108/JEIM-10-2014-0105

23. Barishpolec V. A. Informacionno-psihologicheskaya bezopasnost: osnovnye polozheniya [Information-psychological security: main principles]. *Informacionnye tehnologii*, 2003, vol. 3, no. 2, pp. 69–104.

24. Makarenko S. I. Audit bezopasnosti kriticheskoj infrastruktury specialnymi informacionnymi vozdejstviyami [Security audit of critical infrastructure with special information impacts] Saint-Petersburg, Naukoemkie tekhnologii Publ, 2018. 122 p. (in Russian).

25. Makarenko S. I. Informatsionnoe protivoborstvo i radioelektronnaya borba v setetsentricheskikh voinakh nachala XXI veka [Information warfare and electronic warfare to network-centric wars of the early XXI century]. Saint-Petersburg, Naukoemkie tekhnologii Publ, 2017, 546 p. (in Russian).

26. Azhmuhamedov I. M., Machueva D. A., Zholobov D. A. Modelirovanie processa rasprostraneniya informacii v social'nyh setyah [Modeling the process of information distribution in social networks]. *Fundamentalnye issledovaniya*, 2017. no. 5, pp. 9–14 (in Russia).

27. Bukharin S. N., Malkov S. I. K voprosu o matematicheskom modelirovanii informatsionnykh vzaimodeistvii [To the question of mathematical modeling of

information interactions]. *Informatsionnye voiny*, 2010, vol. 2, no. 14, pp. 14–20 (in Russia).

28. Rastorguev S. P. O proiavlenii skrytykh v strukture sistemy predraspolozhennostei [About the development of the latent structure of the system in predisposition]. *Informatsionnye voiny*, 2017, no. 1, pp. 92–97 (in Russia).

29. Novikov V. A., Demikhov E. N. Podkhod k obosnovaniiu upravlencheskikh reshenii na osnove apriornoi istinnosti informatsii [Approach to justification of management decisions on the basis of aprior true information] // *Naukoemkie tekhnologii v kosmicheskikh issledovaniiakh Zemli*, 2018, vol. 10, no. 5, pp. 75–80 (in Russia).

30. Khlobystova A., Abramov M., Tulupyev A. An Approach to Estimating of Criticality of Social Engineering Attacks Traces. *International Conference on Information Technologies* – Springer, Cham, 2019, vol. 199, pp. 446–456. doi: 10.1007/978-3-030-12072-6_36

31. Khlobystova A. O., Abramov M. V., Tulupyev A. L., Zolotin A. A. Poisk kratchaishei traektorii socioinjenernoi ataki mejdu paroi polzovatelei v grafe s veroyatnostyami perekhodov [Search for the shortest trajectory of a social engeneering attack between a pair of users in a graph with transition probabilities]. *Informatsionno-upravliaiushchie sistemy*, 2018, no. 6, pp. 74–81. doi: 10.31799/1684-8853-2018-6-74-81(in Russian).

Статья поступила 15 августа 2019 г.

Информация об авторах

Хлобыстова Анастасия Олеговна – младший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики. Санкт-Петербургский институт информатики и автоматизации. Область научных интересов: информационная безопасность, социоинженерные атаки, многоходовые социоинженерные атаки, построение профиля уязвимостей пользователя, анализ социальных сетей. E–mail: aok@dscs.pro

Абрамов Максим Викторович – кандидат технических наук. Руководитель лаборатории теоретических и междисциплинарных проблем информатики, старший научный сотрудник. Санкт-Петербургский институт информатики и автоматизации Российской академии наук. Доцент кафедры информатики. Санкт-Петербургский государственный университет. Область научных интересов: информационная безопасность, социоинженерные атаки, анализ защищённости пользователей информационных систем от социоинженерных атак злоумышленников; анализ распространения информации в социальных сетях на основе моделей, применяемых при анализе защищенности пользователей информационных систем от социоинженерных атак; анализ и моделирование социальных сетей; клиент-серверные технологии; исследование взаимосвязей между контентом, публикуемым пользователями в

социальных сетях, и поведением в офлайн-среде; бизнес-аналитика, социокомпьютинг, бизнес-интеллидженс. E–mail: mva@dscs.pro

Тулупьев Александр Львович – доктор физико-математических наук, профессор. Профессор кафедры информатики. Санкт-Петербургский государственный университет. Главный научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики. Санкт-Петербургский институт информатики и автоматизации Российской академии наук. Область научных интересов: представление и обработка данных и знаний с неопределенностью, Data Science, Information Science, применение методов математики и информатики в социокультурных исследованиях, вероятностные графические модели, байесовские сети и родственные модели, применение методов биостатистики и математического моделирования в эпидемиологии. E–mail: alt@dscs.pro

Адрес: 199178, Россия, г. Санкт-Петербург, 14-я линия В.О., д. 39.

Maximum likelihood estimation methods of social engineering attack trajectories detection and information system compromised users revelation

A. O. Khlobystova, M. V. Abramov, A. L. Tulupyev

Purpose. *Nowadays, one of the most important issues of information security for organizations is increasing number of successful social engineering attacks. Significant feature of such attacks is the complexity of related incidents investigation. Currently, there are methods for investigating information secure incidents, which occurs due to use by malefactors hardware-software vulnerabilities, however, there are no similar widely used tools if social engineering attacks incident happens.* ***The aim of the work*** *is to develop maximum likelihood estimation methods, which are directed to detect social engineering attack trajectories and information system compromised users. It facilitates the investigations of social engineering attacks.* ***Methods.*** *A probabilistic approach to assess the degree of user vulnerability to social engineering attacks, an organization information system graph model, which represents user profiles and relations between them, and, also, the critical user documents are used.* ***The novelty of the work*** *is the capability to take into account the susceptibility of staff to social engineering impact, in contrast to earlier investigations of information security incidents, which were based only on technical characteristics. The article proposes an approach, based on probabilistic assessment of single-running and multi-running social engineering attacks which rely, for example, on user vulnerabilities.* ***The result of the work*** *is the approach which helps to conduct an initial investigations of information security incidents which belong to social engineering attacks. The approach is based on maximum likelihood method, which detects social engineering attack trajectories and reveals information system compromised users. The approach is based on the analysis of the social graph of the organization employees and the probabilistic graphical model.* ***The practical significance*** *of the results lies in the development of a tool for decision-makers, which makes it possible to reduce the search space when incidents related to successful social engineering attack implementation are investigated; to minimize the time needed to investigate crimes; to define the basis for the subsequent development of recommender system which reduce the social engineering attacks implementation risk.*

Key words: *social engineering attacks, psychological information impact, backtracking incidents, investigation attacks, trajectories of the spread, information security, user protection, user vulnerability, social networks, social graph.*

Information about Authors

Anastasiia Olegovna Khlobystova – Junior Research Associate of Laboratory of Theoretical and Interdisciplinary Problems of Informatics. St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia. Field of research: information security, social engineering attacks, multiway social engineering attacks, building user vulnerability profile, social network analysis. E–mail:
aok@dscs.pro

Maxim Victorovich Abramov – PhD of Eng. Sci. Senior Research Associate and head of Theoretical and Interdisciplinary Problems of Informatics. St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences. Associate Professor of Computer Science Department. Saint Petersburg State University. Field of research: information security, social engineering attacks, analysis of users security of information systems from social engineering attacks of malefactor; analysis of information dissemination in social networks based on models, which used in the analysis of users security from social engineering attacks; analysis and modeling of social networks; client–server technology; the relation between content published by users in social networks and offline behavior; business analytics, social computing, business intelligence. E–mail: mva@dscs.pro

Alexander Lvovich Tulupyev – Dr. Sci. (Phys. and Math.), Professor. Professor of Computer Science Department. Saint Petersburg State University. Principal Research Associate of Laboratory of Theoretical and Interdisciplinary Problems of Informatics. St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences. Field of research: representation and processing of data and knowledge with indetermination, Data Science, Information Science, application of mathematics and computer science methods in sociocultural research, probabilistic graphical model, Bayesian network and related models, application of biostatistics and mathematical modeling methods in epidemiology. E–mail: alt@dscs.pro

Address: Russia, 199178, Saint-Petersburg, Line 14, 39.