УДК 614.8 + 002.6:004.89

А.А. Азаров, А.Л. Тулупьев, Н.Б. Соловцов, Т.В. Тулупьева

УСКОРЕНИЕ РАСЧЕТОВ ОЦЕНКИ ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЗА СЧЕТ ЭЛИМИНАЦИИ МАЛОВЕРОЯТНЫХ ТРАЕКТОРИЙ СОЦИО-ИНЖЕНЕРНЫХ АТАК

Азаров А.А., Тулупьев А.Л., Соловцов Н.Б., Тулупьева Т.В. **Ускорение расчетов оценки защищенности пользователей информационной системы за счет элиминации маловероятных траекторий социо-инженерных атак.**

Аннотация. Для обеспечения деятельности специалистов в области информационной безопасности необходимо разработать научно-обоснованные и отражающие специфику предметной области математические методы и модели, позволяющие автоматизировать анализ защищенности пользователей информационных систем от социо-инженерных атак. Целью настоящей работы является рассмотрение метода поиска вероятности успеха социо-инженерного атакующего воздействия на каждого пользователя в комплексе «персонал - информационная система – критичные документы», пользователи которого и связи между ними представлены виде графа. Алгоритм предполагает поиск всевозможных ациклических путей между двумя пользователями.

Ключевые слова: социо-инженерная атака, информационная система, пользователь, траектория социо-инженерной атаки.

Azarov A.A., Tulupyev A.L., Solovtsov N.B., Tulupyeva T.V. **Acceleration of calculation of an estimate of information system user's security at the expense of improbable ways of socio-engineering attacks elimination.**

Abstract. In the field of information security it is necessary to develop scientific and proved and mathematical methods and the models reflecting specifics of subject domain for ensuring activity of experts, allowing to automate the analysis of information systems user's security from socio-engineering attacks. The purpose of this paper is consideration of a method of of success probability search of socio-engineering attacking impact on each user in the "personnel - information system - critical documents" complex where users and communications between them are presented as graph. The algorithm assumes search of various acyclic ways between two users.

Keywords: socio-engineering attack, informational system, user, socio-engineering attack way.

1. Введение. Защита конфиденциальной информации неразрывно связана как с программно-технической защищенностью информационных систем, так и с защищенностью пользователей таких систем от негативного влияния социоинженеров извне. Вопросу анализа защищенности программно-технической составляющей информационных систем посвящено немало внимания [6, 21, 22–28], в то время как анализ защищённости пользователей информационных систем от социоинженерных (социотехнических) атак находится на ранней стадии исследований [1–4, 13–16]. Для обеспечения деятельности специалистов в области информационной безопасности необходимо разработать

научно-обоснованные и отражающие специфику предметной области математические методы и модели, позволяющие автоматизировать анализ защищенности пользователей информационных систем от социо-инженерных (социотехнических) атак.

Целью настоящей работы является рассмотрение метода поиска вероятности успеха социо-инженерного атакующего воздействия на каждого пользователя в комплексе «персонал - информационная система – критичные документы» [1–4, 13–16], пользователи которого и связи между ними представлены виде графа [5. 7. 9–12, 17–20]. Алгоритм предполагает поиск всевозможных ациклических путей между двумя пользователями. Также будет приведена иллюстрация метода расчета полной вероятности системы на упрощенном (для доступности и краткости изложения) примере.

2. Вероятность успешной реализации атаки на пользователя. Подсчет вероятности ответных действий определенных пользователей сети на социо-инженерные атакующие воздействия злоумышленника позволяет судить о защищенности данного «узла» системы, то есть пользователя, но не о защищенности системы в целом. Для подсчета совокупной вероятности защищенности информационной системы от социо-инженерных атак злоумышленника можно пользоваться несколькими эвристиками. В настоящей работе предложен подход к подсчету такой вероятности, сводящийся к поиску всевозможных путей в графе и последующей комбинации весов их рёбер. Общая схема ключевых шагов подобного алгоритма выглядит следующим образом. Изначально у злоумышленника есть один кандидат для атаки. Для удобства, не умаляя общности, присвоим ему номер один. После этого предполагаем, что у любого из пользователей может оказаться доступ к требуемому злоумышленнику файлу, и ищем вероятности успешности социо-инженерной атаки злоумышленника на каждого пользователя, учитывая при этом веса перехода (веса рёбер) от пользователя к пользователю; причём веса вероятность успеха установления контакта злоумышленника со вторым пользователем.

На рис. 1 представлен пример графа, представляющего сложившиеся социальные связи персонала информационной системы. Каждому узлу графа соответствует пользователь информационной системы. Поэтому вес узла — вероятность успешности социо-инженерного атакующего воздействия злоумышленника на того пользователя, которому соответствует данный узел графа. В данном случае, под вероятностью успешности социо-инженерного атакующего воздействия злоумышленника понимается совокупная вероятность успешности социо-

инженерной атаки на пользователя в случае применения всех атакующих воздействий. Ребру графа соответствуют взаимоотношения между пользователями. Каждое ребро графа, то есть связь между пользователями, имеет собственный вес, который соответствует вероятности успешного перехода по этой связи в случае социо-инеженерного воздействия злоумышленника. В данном графе мы рассматриваем двунаправленные связи ради упрощения рассматриваемой модели. Вообще говоря, в реальной ситуации, при анализе защищенности пользователей, связи между двумя пользователями односторонни и, переходя к графовой структуре, каждая из них имеет свою вероятность успешного перехода в случае социо-инженерного воздействия злоумышленника.

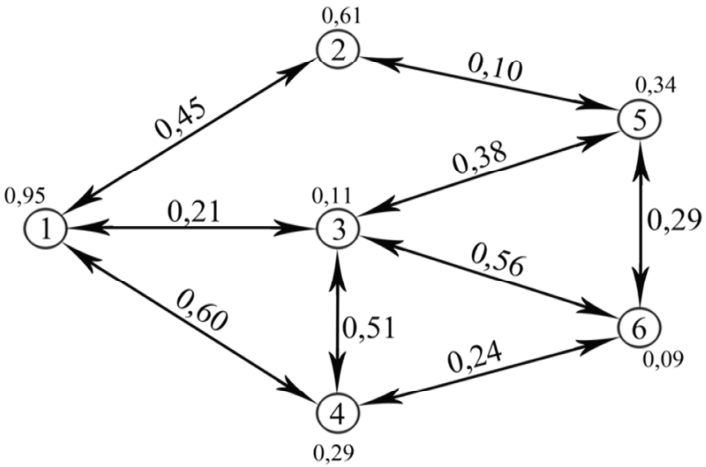

Рис. 1. Пример графа социальных связей персонала информационной системы.

Пусть P_i — вероятность успешности атаки на i-того сотрудника, если у злоумышленника есть на него выход. $P_{i,j}$ — вероятность выхода злоумышленника на пользователя j через пользователя i если пользователь i уже успешно атакован. Тогда вероятность успешного выхода злоумышленника на пользователя j через путь, проходящий через пользователей i_k и начинающийся с пользователя m: $\tilde{P}_{m-\cdots-i_k-\cdots-j} = P_m \prod_{k=1}^{n-1}(P_{i_k,i_{k+1}} P_{i_{k+1}})$, где $i_1 = m, i_n = j$. Теперь, когда у нас есть вероятность успешного выхода злоумышленника на пользователя j через цепь пользователей, вычислим формулу атаки через несколько цепей

пользователей $\tilde{P}_i$: $\tilde{P}_{sum\ j} = 1 - \sum_{i=1..k}(\tilde{P}_i)$. Соответственно чтобы $\tilde{P}_{\text{sum } j}$ была полной вероятностью успеха атаки на пользователя j, нужно, чтобы цепи были полным дизъюнктивным (с точки зрения теории вероятностей) множеством всевозможных путей, либо аппроксимировали его.

3. Преимущества и недостатки рассматриваемого подхода. В настоящей работе предложен эвристический подход, при котором учитываются всевозможные пути в графе отношений пользователей, не содержащие циклов. Преимуществами такого подхода является то, что он позволяет рассчитать именно искомую вероятность успеха социо-инженерной атаки злоумышленника на пользователя информационной системы через сеть пользователей, а также прост в понимании, поскольку, фактически, сводится к формуле суммы вероятностей дизъюнктных событий. В то же время при больших объемах данных, возникает огромное число цепей с небольшим весом (то есть соответствующих ничтожно малой вероятности успешного выхода злоумышленника на атакуемого пользователя). Кроме того, для каждого из пользователей вероятность его «поражения», «успеха социо-инженерной атаки» нужно рассчитывать отдельно.

Подчеркнем пару особенностей предложенного подхода.

Свойство 1. Вероятность успеха атаки на пользователя зависит в большей степени от минимальной длины цепочки, которую можно построить между первой жертвой злоумышленника и атакуемым пользователем.

Свойство 2. Вероятности успешных переходов по длинным цепочкам ничтожно малы по сравнению с вероятностями, вычисленными для более коротких цепочек, соответственно, они вносят малозаметный вклад в итоговую оценку.

Определение. Длинными будем называть цепочки, вероятность успешного социо-инженерного атакующего воздействия по которым меньше, скажем 1%, а также получающиеся из них путем добавления новых узлов.

На основании данных свойств можно предложить критерий отброса длинных цепочек, имеющих ничтожно малый вес в конечном результате.

Критерий. Рассматривать можно только цепочки минимальной длины и цепочки, длина которых больше этой длины на два–три звена. При этом из рассмотрения следует исключить более длинные цепочки.

При применении данного критерия работа алгоритма на больших объемах данных значительно ускоряется в силу рассмотрения меньшего числа вариантов развития социо-инженерных атак.

4. Пример реализации. Рассмотрим схему взаимоотношений пользователей, взятых со случайными данными, описанную на рис.1. Как мы уже договорились, злоумышленник начинает атаку с первого пользователя. Рассчитаем вероятность атаки на второго пользователя: атака может происходить по цепям: 1-2; 1-3-5-2; 1-3-6-5-2; 1-3-4-6-5-2; 1-4-3-5-2; 1-4-3-6-5-2; 1-4-6-3-5-2; 1-4-6-5-2. Разберем подробнее, как рассчитывается цепь 1-4-3-5-2. $\widetilde{P}_{1-4-3-5-2} = P_1P_{1,4}P_4P_{4,3}P_3P_{3,5}P_5P_{5,2}P_2 = 0{,}95 \cdot 0{,}60 \cdot 0{,}29 \cdot 0{,}51 \cdot 0{,}11 \cdot 0{,}38 \cdot 0{,}34 \cdot 0{,}10 \cdot 0{,}61 = 0.000073085.$

$\widetilde{P}_{1-2} = 0{,}26078,$ $\widetilde{P}_{1-3-4-6-5-2} = 0{,}00000,$ $\widetilde{P}_{1-4-6-3-5-2} = 0{,}00000,$

$\widetilde{P}_{1-3-5-2} = 0{,}00017,$ $\widetilde{P}_{1-4-3-5-2} = 0{,}00007,$ $\widetilde{P}_{1-4-6-5-2} = 0{,}00002,$

$\widetilde{P}_{1-3-6-5-2} = 0{,}00001,$ $\widetilde{P}_{1-4-3-6-5-2} = 0{,}00000,$ $\widetilde{P}_{\text{sum }2} = 0{,}26098,$

$\widetilde{P}_{1-3} = 0{,}26098,$ $\widetilde{P}_{1-2-5-6-4-3} = 0{,}00001,$ $\widetilde{P}_{1-4-6-5-3} = 0{,}00000,$

$\widetilde{P}_{1-2-5-3} = 0{,}02195,$ $\widetilde{P}_{1-4-3} = 0{,}00927,$ $\widetilde{P}_{\text{sum }3} = 0{,}03162,$

$\widetilde{P}_{1-2-5-6-3} = 0{,}00037,$ $\widetilde{P}_{1-4-6-3} = 0{,}00001,$

$\widetilde{P}_{1-4} = 0{,}16530,$ $\widetilde{P}_{1-2-5-6-4} = 0{,}00002,$ $\widetilde{P}_{1-3-6-4} = 0{,}00000,$

$\widetilde{P}_{1-2-5-3-4} = 0{,}00005,$ $\widetilde{P}_{1-3-4} = 0{,}00325,$ $\widetilde{P}_{\text{sum }4} = 0{,}16814,$

$\widetilde{P}_{1-2-5-3-6-4} = 0{,}00000,$ $\widetilde{P}_{1-3-5-6-4} = 0{,}00001,$

$\widetilde{P}_{1-2-5} = 0{,}00887,$ $\widetilde{P}_{1-3-6-5} = 0{,}00011,$ $\widetilde{P}_{1-4-6-5} = 0{,}00035$

$\widetilde{P}_{1-3-5} = 0{,}00284,$ $\widetilde{P}_{1-4-3-5} = 0{,}00120,$ $\widetilde{P}_{1-4-6-3-5} = 0{,}00003,$

$\widetilde{P}_{1-3-4-6-5} = 0{,}00001,$ $\widetilde{P}_{1-4-3-6-5} = 0{,}00005,$ $\widetilde{P}_{\text{sum }5} = 0{,}01340,$

$\widetilde{P}_{1-2-5-6} = 0{,}00023,$ $\widetilde{P}_{1-3-4-6} = 0{,}00007,$ $\widetilde{P}_{1-4-3-5-6} = 0{,}00003.$

$\widetilde{P}_{1-2-5-3-6} = 0{,}00002,$ $\widetilde{P}_{1-3-5-6} = 0{,}00007,$ $\widetilde{P}_{\text{sum }6} = 0{,}00556,$

$\widetilde{P}_{1-2-5-3-4-6} = 0{,}00000,$ $\widetilde{P}_{1-4-6} = 0{,}00357,$

$\widetilde{P}_{1-3-6} = 0{,}00111,$ $\widetilde{P}_{1-4-3-6} = 0{,}00047,$

По итогам работы рассмотренного подхода консолидированная вероятность успешной социо-инженерной атаки на пользователей составляет соответственно:

$\widetilde{P}_{\text{sum }2} = 0{,}26098,$

$\widetilde{P}_{\text{sum }3} = 0{,}03162,$

$\widetilde{P}_{sum\ 4} = 0{,}16814,$
$\widetilde{P}_{sum\ 5} = 0{,}01340,$
$\widetilde{P}_{sum\ 6} = 0{,}00556.$

5. Заключение. В настоящей работе рассмотрен подход к вычислению оценки вероятности успеха социо-инженерного атакующего воздействия на каждого пользователя в комплексе «персонал – информационная система – критичные документы», представленного в виде графа (для изложения основных принципов было достаточно ограничиться графом социальных связей пользователей). Предложенный подход сводится к поиску всевозможных ациклических путей между двумя пользователями в графе. Выделены особые свойства подхода, на основе которых предложен критерий, позволяющий уменьшить вычислительную сложность поиска полной вероятности успеха социо-инженерного атакующего воздействия на пользователя информационной системы. Следует отметить, что на практике может потребоваться критерий, более тонко характеризующий «длинные» цепочки и «малые вероятности»; однако такая «настройка» критерия будет в значительной степени определяться конкретной ситуацией. Принцип же оптимизации вычислений за счет отброса особо длинных цепочек с особо малыми вероятностями успеха реализации атакующих действий в таком случае останется неизменным.

Литература

1. *Азаров А.А., Тулупьева Т.В., Фильченков А.А., Тулупьев А.Л.* Вероятностно-реляционный подход к представлению модели комплекса «Информационная система – персонал – критичные документы». // Труды СПИИРАН. 2012. Вып. 20. С. 57–71.
2. *Азаров А.А., Тулупьева Т.В., Тулупьев А.Л.* Прототип комплекса программ для анализа защищенности персонала информационных систем построенный на основе фрагмента профиля уязвимостей пользователя. // Труды СПИИРАН. 2012. Вып. 21. С. 21–40.
3. *Азаров А.А., Тулупьев А.Л., Тулупьева Т.В.* SQL-представление реляционно-вероятностных моделей социо-инженерных атак в задачах расчета агрегированных оценок защищенности персонала информационной системы // Труды СПИИРАН. 2012. Вып. 22. С. 31–44.
4. *Ванюшичева О.Ю.* Прототип комплекса программ для построения профиля психологически обусловленных уязвимостей пользователя. Дипломная работа. СПб.: СПбГУ, 2012.
5. *Зельтерман Д., Суворова А.В., Пащенко А.Е., Мусина В.Ф., Тулупьев А.Л., Тулупьева Т.В., Гро Л.Е., Хаймер Р.* Диагностика регрессионных уравнений в анализе интенсивности рискованного поведения по его последним эпизодам // Труды СПИИРАН. 2011. Вып. 17. С. 33–46.
6. *Котенко И.В., Юсупов Р.М.* Перспективные направления исследований в области компьютерной безопасности. Защита информации. Инсайд. 2006. № 2. С. 46.

7. *Пащенко А.Е., Тулупьев А.Л., Суворова А.В., Тулупьева Т.В.* Сравнение параметров угрозообразующего поведения в разных группах на основе неполных и неточных данных // Труды СПИИРАН. 2009. Вып. 8. СПб.: Наука, 2009. С. 252–261.
8. *Петренко С.А.* Возможная методика построения системы информационной безопасности предприятия. // URL: http://bre.ru/security/13985.html (дата обращения 10.01.12)
9. *Пинский М.Я., Сироткин А.В., Тулупьев А.Л., Фильченков А.А.* Повышение быстродействия алгоритма оценки наблюдаемой последовательности в скрытых марковских моделях на основе алгебраических байесовских сетей // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2011. Вып. 5. С. 69–73.
10. *Сироткин А.В., Тулупьев А.Л., Фильченков А.А., Пащенко А.Е., Тулупьева Т.В., Мусина В.Ф.* Особенности вероятностных графических моделей комплекса «Информационная система–персонал» для оценки его защищенности от социоинженерных атак // Научная сессия НИЯУ МИФИ-2011. (1–5 февраля 2011 г., Москва.)Аннотации докладов. В 3 т. Т. 3: Стратегические информационные технологии в атомной энергетике и промышленности. Проблемы информационной безопасности в системе высшей школы. Экономические и правовые проблемы инновационного развития атомной отрасли. Образование в Национальном исследовательском ядерном университете. М.: НИЯУ МИФИ, 2011. С. 80.
11. *Суворова А.В., Тулупьев А.Л., Пащенко А.Е., Тулупьева Т.В., Красносельских Т.В.* Анализ гранулярных данных и знаний в задачах исследования социально значимых видов поведения // Компьютерные инструменты в образовании. №4. 2010. С. 30–38.
12. *Суворова А.В., Пащенко А.Е., Тулупьева Т.В.* Оценка характеристик сверхкороткого временного ряда по гранулярным данным о рекордных интервалах между событиями // Труды СПИИРАН. 2010. Вып. 12. С. 170–181.
13. *Тулупьев А.Л., Азаров А.А., Тулупьева Т.В., Пащенко А.Е., Степашкин М.В.* Социально-психологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социоинженерных атак // Труды СПИИРАН. 2010. Вып. 1 (12). С. 200–214.
14. *Тулупьев А.Л., Азаров А.А., Пащенко А.Е.* Информационные модели компонент комплекса «Информационная система – персонал», находящегося под угрозой социоинженерных атак // Труды СПИИРАН. 2010. Вып. 3 (14). С. 50–57.
15. *Тулупьев А.Л., Азаров А.А., Тулупьева Т.В., Пащенко А.Е., Степашкин М.В.* Генерализация моделей деревьев атак на случай социоинженерных атак // Научная сессия МИФИ-2011. Аннотации докладов. В 3 т. Т. 3. М.: МИФИ, 2011. С. 89.
16. *Тулупьева Т.В., Тулупьев А.Л., Азаров А.А., Пащенко А.Е.* Психологическая защита как фактор уязвимости пользователя в контексте социоинженерных атак // Труды СПИИРАН. 2011. Вып. 18. С. 74–92.
17. *Тулупьев А.Л., Фильченков А.А., Вальтман Н.А.* Алгебраические байесовские сети: задачи автоматического обучения // Информационно-измерительные и управляющие системы. 2011. № 11, т. 9. С. 57-61.
18. *Фильченков А.А., Тулупьев А.Л.* Совпадение множеств минимальных и нередуцируемых графов смежности над первичной структурой алгебраической байесовской сети // Вестник Санкт-Петербургского государственного университета. Серия 1. Математика. Механика. Астрономия. 2012. Вып. 2. С. 65–74.
19. *Фильченков А.А., Тулупьев А.Л., Сироткин А.В.* Структурный анализ клик максимальных графов смежности алгебраических байесовских сетей // Вестн. Тверск. гос. ун-та. Сер.: Прикладная математика. 2011. №20. С. 139–151.

20. *Фильченков А.А., Тулупьев А.Л.* Анализ циклов в минимальных графах смежности алгебраических байесовских сетей // Труды СПИИРАН. 2011. Вып. 2 (17). С. 151–173.
21. *Юсупов Р., Пальчун Б.П.* Безопасность компьютерной инфосферы систем критических приложений. Вооружение. Политика. Конверсия. 2003. № 2. С. 52.
22. *Dorothy D.E.* A Lattice Model of Secure Information Flow // Communications of the ACM. 2008. Vol. 19.No. 5. p. 236–243.
23. *Balepin I., Maltsev S., Rowe, J., Levitt K.* Using specification-based intrusion detection for automated response //Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection. 2003. p. 135-154.
24. *Jahnke M., Thul C., Martini P.* Graph based metrics for intrusion response measures in computer networks //LCN 2007: Proceedings of the 32nd IEEE Conferenceon Local Computer Networks. IEEE Computer Society, LosAlamitos. 2007. Washington. DC. USA. p. 1035-1042.
25. National Institute of Standards and Technology. URL: http://www.nist.gov/index.html (дата обращения 24.06.2012)
26. Siemens. The total information security toolkit. URL: http://www.cramm.com/(дата обращения 24.06.2012)
27. Software Engineering Institute. URL: http://www.cert.org/octave/ (дата обращения 24.06.2012)
28. *Toth T., Krugel C.* Evaluating the impact of automated intrusion response mechanisms //ACSAC 2002: Proceedings of the 18th Annual Computer Security Applications Conference. IEEE Computer Society, Los Alamitos. 2002. Washington. DC. USA. p. 301.

Азаров Артур Александрович — м.н.с., лаборатория теоретических и междисциплинарных проблем информатики, СПИИРАН. Область научных интересов: защита информации, анализа защищенности информационных систем. Число научных публикаций — 42. Artur-azarov@yandex.ru, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Azarov Artur Alexandrovich — junior researcher, Laboratory of Theoretical and Interdisciplinary Computer Science, SPIIRAS. Research interests: information protection, information system's protection analysis. The number of publications — 42. Artur-azarov@yandex.ru, www.tulupyev.spb.ru; SPIIRAS, 39, 14-thLine V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Тулупьев Александр Львович — д-р физ.-мат. наук., доцент; заведующий лабораторией теоретических и междисциплинарных проблем информатики СПИИРАН, доцент кафедры информатики математико-механического факультета СПбГУ. Область научных интересов: представление и обработка данных и знаний с неопределенностью, применение методов математики и информатики в социокультурных и эпидемиологических исследованиях, технология разработки программных комплексов с СУБД. Число научных публикаций — 200. ALT@iias.spb.su, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Tulupyev Alexander Lvovich — Dr. Sc. in Physics and Mathematics, associate professor; head of Laboratory of Theoretical and Interdisciplinary Computer Science, SPIIRAS, associate professor, Computer Science Department, Faculty of Mathematics and Mechanics, SPbSU. Research interests: uncertain knowledge and data representation and processing, application of mathematics and computer science in socio cultural and epidemiological studies, software

technologies and development of information systems with databases. The number of publications — 200.ALT@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14-thLine V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Соловцов Никита Борисович — студент кафедры информатики, математико-механический факультет СПбГУ. Область научных интересов: защита информации, анализ защищенности информационных систем. Число научных публикаций — 1. Nekit.tg@gmail.com; СПбГУ, СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Solovtsov Nikita Borisovich — student, Department of Computer Science, faculty of mathematics and mechanics, SPbSU. Research interests: information protection, information system's protection analysis. The number of publications — 1. Nekit.tg@gmail.com; SPbSU, SPIIRAS, 39, 14-thLine V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Тулупьева Татьяна Валентиновна — доцент, канд. психол. наук; с. н. с. Лаборатории теоретических и междисциплинарных проблем информатики, СПИИРАН. Область научных интересов: применение методов математики и информатики в гуманитарных исследованиях, информатизация организации и проведения психологических исследований, применение методов биостатистики в эпидемиологии, психология личности, психология управления Число научных публикаций — 80. TVT@iias.spb.su, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Tulupyeva Tatiana Valentinovna — associate professor, PhD in Psychology; senior researcher, Theoretical and Interdisciplinary Computer Science Laboratory, SPIIRAS. Research interests: application of mathematics and computer science in humanities, informatization of psychological studies, application of biostatistics in epidemiology, psychology of personality, management psychology The number of publications — 80. TVT@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14-thLine V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Поддержка исследований. Исследование поддержано грантом РФФИ на 2010–2012 гг., проект № **10-01-00640-а**, грантом СПбГУ на 2011–2013 гг., проект № **6.38.72.2011**., Грант РФФИ на 2012–2014 гг., проект № **12-01-00945-а**, стипендия Правительства Российской федерации (пр. 874 от 29.10.2012).

Рекомендовано лабораторией теоретических и междисциплинарных проблем информатики, заведующий лабораторией Тулупьев А.Л., д.ф-м.н., доц.
Статья поступила в редакцию 10.02.2013.

РЕФЕРАТ

Азаров А.А., Тулупьев А.Л., Соловцов Н.Б. Тулупьева Т.В. **Ускорение расчетов оценки защищенности пользователей информационной системы за счет элиминации маловероятных траекторий социо-инженерных атак.**

Защита конфиденциальной информации неразрывно связана как с программно-технической защищенностью информационных систем, так и с защищенностью пользователей таких систем от негативного влияния социо-инженеров извне. Вопросу анализа защищенности программно-технической составляющей информационных систем посвящено немало внимания, в то время как анализ защищённости пользователей информационных систем от социо-инженерных (социотехнических) атак находится на ранней стадии исследований. Для обеспечения деятельности специалистов в области информационной безопасности необходимо разработать научно-обоснованные и отражающие специфику предметной области математические методы и модели, позволяющие автоматизировать анализ защищенности пользователей информационных систем от социо-инженерных (социотехнических) атак.

Целью настоящей работы является рассмотрение метода поиска вероятности успеха социо-инженерного атакующего воздействия на каждого пользователя в комплексе «персонал - информационная система – критичные документы», пользователи которого и связи между ними представлены виде графа. Алгоритм предполагает поиск всевозможных ациклических путей между двумя пользователями. Также будет приведена иллюстрация метода расчета полной вероятности системы на упрощенном (для доступности и краткости изложения) примере.

В настоящей работе рассмотрен подход к вычислению оценки вероятности успеха социо-инженерного атакующего воздействия на каждого пользователя в комплексе «персонал – информационная система – критичные документы», представленного в виде графа (для изложения основных принципов было достаточно ограничиться графом социальных связей пользователей). Предложенный подход сводится к поиску всевозможных ациклических путей между двумя пользователями в графе. Выделены особые свойства подхода, на основе которых предложен критерий, позволяющий уменьшить вычислительную сложность поиска полной вероятности успеха социо-инженерного атакующего воздействия на пользователя информационной системы. Следует отметить, что на практике может потребоваться критерий, более тонко характеризующий «длинные» цепочки и «малые вероятности»; однако такая «настройка» критерия будет в значительной степени определяться конкретной ситуацией. Принцип же оптимизации вычислений за счет отброса особо длинных цепочек с особо малыми вероятностями успеха реализации атакующих действий в таком случае останется неизменным.

SUMMARY

Azarov A.A., Tulupyev A.L., Solovtsov N.B., Tulupyeva T.V. **Acceleration of calculation of an estimate of information system user's security at the expense of improbable ways of socio-engineering attacks elimination.**

Protection of confidential information is inseparably linked as with about program-technical security of information systems, and with security of users of such systems from negative influence of socio engineer from the outside. A lot of attention is pay to the analysis of a program and technical component security of information systems, while the analysis of information systems user's security from socio-engineering attacks is at an early stage of researches. In the field of information security it is necessary to develop scientific and proved and mathematical methods and the models reflecting specifics of subject domain for ensuring activity of experts, allowing to automate the analysis of information systems user's security from socio-engineering (sociotechnical) attacks.

The purpose of this paper is consideration of a method of success probability search of socio-engineering attacking impact on each user in the "personnel - information system - critical documents" complex where users and communications between them are presented as graph. The algorithm assumes search of various acyclic ways between two users. Also the illustration of a method of a total probability calculation of system on simplified (for availability and brevity statement) an example will be given.

In the real work approach to calculation of an assessment of probability of success of socio-engineering attacking impact on each user in the "personnel-information system-critical documents" complex, presented in the form of the count (for a statement of the basic principles was enough it will be limited to the count of social communications of users) is considered. The offered approach is reduced to search of various acyclic ways between two users in the column. Special characteristics of approach on the basis of which the criterion, allowing to reduce computing complexity of search of a total probability of success of socio-engineering attacking impact on the user of information system is offered are allocated. It should be noted that in practice the criterion can be demanded, is thinner characterizing "long" chains and "small probabilities"; however such "control" of criterion will be defined substantially by a concrete situation. The principle of optimization of calculations for the account elimination especially long chains with especially small probabilities of success of realization of attacking actions in that case remains invariable.