УДК614.8 + 002.6:004.89

А.А. Азаров

АНАЛИЗ ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ГРАФИЧЕСКИХ МОДЕЛЕЙ, СОДЕРЖАЩИХ ПРОФИЛИ УЯЗВИМОСТЕЙ

Азаров А.А. **Анализ защищенности пользователей информационных систем на основе графических моделей, содержащих профили уязвимостей.**
Аннотация. Проблема защиты критичной информации в настоящее время является одной из самых актуальных в информационных технологиях, хотя нельзя не признать, что, с исторической точки зрения, близкородственные ей проблемы зародились гораздо раньше — видимо, одновременно с возникновением письменности. Общепринятый подход к решению данных проблем заключается в развитии, диверсификации и усложнении применяемых технических мер обеспечения безопасности. Таким образом минимизируются возможности технических атак на системы. В то же время, каждая защищаемая информационная система имеет санкционированных пользователей, которые на законных основаниях работают в ней и зачастую имеют легальный доступ к конфиденциальной информации. Целью данной статьи является построение алгоритма анализа резистентности пользователей информационных систем от социо-инженерных атак с учетом профиля уязвимостей пользователя.
Ключевые слова: социо-инженерная атака, информационная система, пользователь, профиль уязвимостей пользователя, резистентность пользователя.

Azarov A.A. **Information systems' user's protection analysis on the basis of the graphic models containing user's vulnerabilities profile.**
Abstract. The problem of critical information protection is now one of the most actual in information technologies though it is necessary to recognize that, from the historical point of view, closely related to it problems arose much earlier — probably, at the same time with writing emergence. The standard approach to the solution of these problems consists in development, diversification and complication of applied technical measures of safety. Thus possibilities of technical attacks to systems are minimized. At the same time, each protected information system has the authorized users who work at the lawful bases in it and often have legal access to confidential information. The purpose of this article is creation of an analysis algorithm of resistance of users of information systems from socio-engineering attacks taking into account a profile of vulnerabilities of the user.
Keywords: socio-engineering attack, informational system, user, user's vulnerabilities profile, user's resistance.

1. Введение. Проблема защиты критичной информации в настоящее время является одной из самых актуальных в информационных технологиях, хотя нельзя не признать, что, с исторической точки зрения, близкородственные ей проблемы зародились гораздо раньше — видимо, одновременно с возникновением письменности. Общепринятый подход к решению данных проблем заключается в развитии, диверсификации и усложнении применяемых технических мер обеспечения безопасности. Таким образом минимизируются возможности

технических атак на системы [5, 7, 20, 21–27]. В то же время, каждая защищаемая информационная система имеет санкционированных пользователей, которые на законных основаниях работают в ней и зачастую имеют легальный доступ к конфиденциальной информации. Проблема разграничения доступа к конфиденциальной информации разбивается на несколько подзадач. Первая задача — это отсечение тех пользователей, которым работа с конфиденциальной информацией не нужна. Подобные вопросы легко решаются изменением политик доступа пользователей к документам. Вторая задача – пользователю требуются определенные критичные документы в его работе. Нельзя ограничить доступ таких пользователей к конфиденциальной информации, так как это может нарушить нормальное течение бизнес-процессов в организации. Наконец возможен третий вариант. Это технические работники, которые тем или иным способом обрабатывают конфиденциальную информацию по поручению своих руководителей. Данные пользователи также подвержены СИ-атакам. В то же время к ним трудно применить ограничение политик доступа, так как задачи работы с конфиденциальными данными возникает постоянно, и, если руководитель будет каждый раз ждать смены политик безопасности, применяемых к его подчиненным, это может привести к серьезным временным затратам, что зачастую недопустимо в современном бизнесе. Таким образом, даже если в организации очень строго расписаны все политики доступа, то все равно существует риск утечки конфиденциальной информации через легальных пользователей информационной системы.

Санкционированные пользователи обладают возможностью повредить или украсть конфиденциальную информацию, что, без сомнения, нанесет существенный урон информационной системе в частности и компании в целом [4, 6]. Данные нелегальные действия пользователя с информацией могут быть вызваны как инсайдерскими атаками, исходящими от самих пользователей, так и социо-инженерными атаками, исходящими от злоумышленников, и направленные на пользователей информационных систем. Так, пользователь, находящийся под влиянием злоумышленника извне, совершает действия, не отдавая себе отчета в том, что они могут нанести вред системе. Таким образом, необходимо анализировать защищенность пользователей от такого рода атак и вырабатывать ряд профилактических мер, с целью предотвращения как социо-инженерных, так и инсайдерских атак. Актуальность данного вопроса обусловлена в первую очередь тем, что анализ защищенности пользователей от социо-инженерных атак неразрывно

связан с анализом защищенности всей информационной системы в целом и хранящихся в ней критических документов в частности.

В статьях [1–3, 11–14] был рассмотрен алгоритм моделирования социо-инженерных атак по рекомпенсационному типу на пользователей информационной системы. Данный алгоритм был адаптацией и развитием алгоритма деревьев атак, предложенным в [11–14] и применявшемуся только по отношению программно-технических сущностей. Затем, в [1–3], был предложен подход к анализу защищенности пользователей информационных систем с применением профиля уязвимостей пользователя. Был предложен алгоритм, который по психологическим особенностям пользователя строит фрагмент профиля его уязвимостей. В данный фрагмент профиля уязвимостей включены 5 уязвимостей пользователя. Получены численные выражения данных уязвимостей. Также выявлен ряд элементарных социо-инженерных воздействий злоумышленника на пользователей информационной системы. Исходя из степени выраженности уязвимостей, содержащихся в профиле уязвимостей пользователя, удалось составить вероятностные оценки резистентности пользователя к конкретным видам социо-инженерных элементарных атакующих воздействий. Таким образом, были получены оценки защищенности конкретного пользователя от социо-инженерных атак без необходимости (или при невозможности) моделирования общей защищенности информационной системы.

Целью данной статьи является построение алгоритма анализа резистентности пользователей информационных систем от социо-инженерных атак на основании объединения первого и второго подходов.

2. Описание предлагаемого подхода к анализу защищенности пользователей информационной системы. К рассмотрению предлагается подход, построенный на объединенной вероятности успешности элементарных социо-инженерных атакующих воздействий злоумышленника [8–11, 16–19]. В дальнейшем планируется адаптация данного подхода к более общему случаю, когда будут рассматриваться отдельные элементарные атакующие воздействия злоумышленника, а также их комбинации.

Рассмотрим комплекс «информационная система – персонал – критические документы». Для того чтобы анализировать защищенность пользователей информационных систем рассмотрим связи между пользователями. Под связями понимаются различные отношения между людьми в организации. При имитации социо-инженерных атакующих воздействий злоумышленника предполагается использование

данных связей в следующем контексте: в случае, если пользователь оказался подвержен СИ-атакующему воздействию злоумышленника, и, в то же время на доступных ему устройствах не обнаружилась требуемая злоумышленнику информация, то происходит переход по связям пользователя к другим пользователям. На новых пользователей будет осуществлено новое СИ-атакующее воздействие. При этом рассматривается также вероятность перехода по связям пользователя. Предполагается, что каждый тип связи обладает собственным «весом», то есть вероятностью того, что злоумышленник сможет воспользоваться этой связью и применить СИ-атакующее воздействие к новому пользователю.

С точки зрения цели работы, предлагается рассматривать модель структуры информационной системы в виде графа (V, E).

В предлагаемой модели пользователи представлены вершинами V, причем существенные свойства пользователей описаны как атрибуты вершин:

- множество устройств, к которым у данного пользователя есть доступ (данный пункт также подразумевает доступ к конфиденциальной информации, которая хранится на данных устройствах);
- права доступа пользователя к конфиденциальной информации;
- должность пользователя;
- права доступа пользователя к контролируемым зонам.

Под множеством дуг E понимается набор связей каждого отдельного пользователя с другими пользователями. В качестве связей были рассмотрено следующее множество: Знакомые, Друзья, Любовь, Родственники, Враги. Здесь приведен пример возможных значений. Типов связи может быть больше, и они могут быть иные.

Каждому элементу из V сопоставлен вес, который отвечает за вероятность успеха социо-инженерных атакующих воздействий на пользователя информационной системы. Обозначим данный вес через p_i, где i — номер пользователя. Каждому элементу из E (u, v) сопоставлен вес, отвечающий за вероятность успеха привлечения пользователя v через пользователя u. Данный вес является единым для каждого элемента из множества связей, которое было приведено выше. Обозначим данный вес через r_{ij}, где i — номер пользователя u, а j — номер пользователя v.

Ключевые шаги алгоритма оценки степени защищенности пользователей информационной системы таковы.

Шаг 0. Зададим итоговую вероятность успеха СИ-атаки, как p_n.

Шаг 1. Происходит выбор пользователя, на которого злоумышленник оказывает первое социо-инженерное атакующее воздействие. В зависимости от успешности данного действия строится оценка вероятности успеха, обозначаемая p_1. Затем, в случае успешной атаки, происходит анализ имеющейся конфиденциальной информации на доступных данному пользователю устройствах. Если требуемая информация найдена, то переход к шагу Выход 1 и $p_n = p_1$. Если нет, то переход к Шагу 2. Изменение статуса данного пользователя на «просмотренный».

Шаг 2. Проверка связей пользователя. Выявление пользователей-соседей. Анализ возможности успешной социо-инженерной атаки на пользователей-соседей. Анализ конфиденциальной информации, на доступных пользователю-соседу устройствам. В случае обнаружения требуемой информации, пользователю-соседу сопоставляется p_2, как вероятность успешности СИ-атаки на этого пользователя. Также связи между первым пользователем и пользователем-соседом сопоставляется r_{12}, как вероятность успеха реализации СИ-атаки через данную связь между пользователями. Итоговая вероятность получения доступа к интересующей злоумышленника конфиденциальной информации составляет $p_1 r_{12} p_2$. Переход к шагу Выход 1 и $p_n = p_1 r_{12} p_2$. В случае, если конфиденциальная информация не найдена, то происходит выбор пользователя соседа в соответствии с формулой $\max_{i=2..k}(p_i)$, где i это порядковый номер пользователя-соседа, а k – количество пользователей-соседей. Изменение статуса выбранного пользователя на «просмотренный». Промежуточная вероятность успешности СИ-атаки $p_{n-1} = p_1 r_{12} p_2$. Затем происходит переход к Шагу 3.

Шаг 3. Аналогично Шагу 2. Различие данных шагов заключается в том, что в данном шаге вместо p_1, использованного в Шаге 1, будет использоваться p_{n-1}.

Выход 1. Конфиденциальная информация доступна злоумышленнику. Вероятность доступа p_n.

Выход 2. Конфиденциальная информация, требуемая злоумышленнику, надежно защищена от известных угроз (имеются ввиду те угрозы, которые описаны в БД системы).

Приведем блок-схему данного алгоритма.

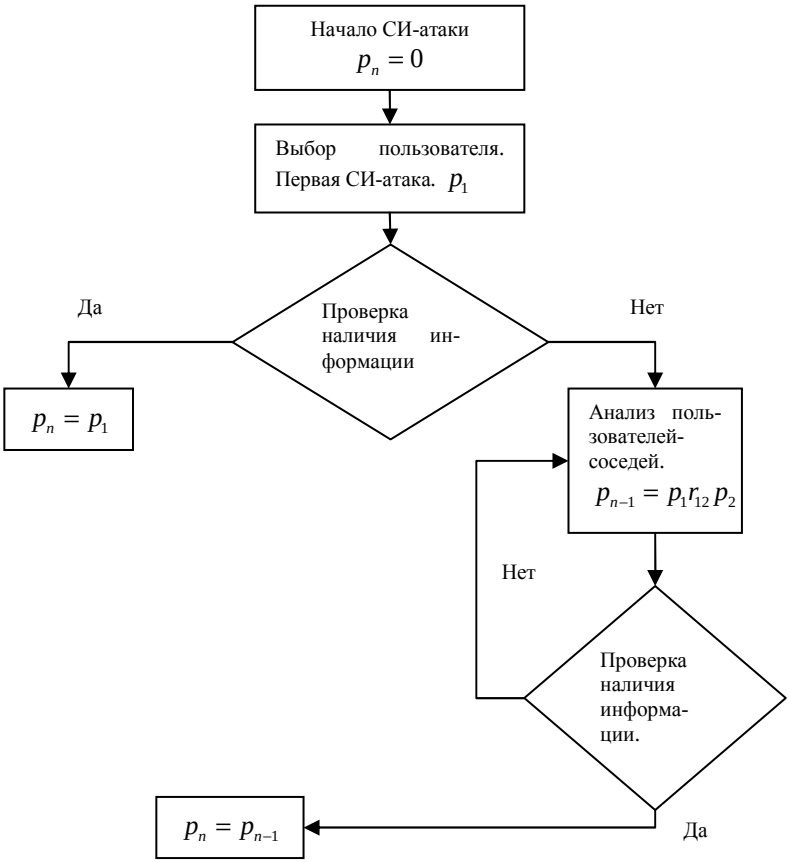

Рис.1. Блок-схема алгоритма анализа защищенности конфиденциальной информации

Данный алгоритм является адаптацией алгоритма Дейкстры поиска кратчайшего пути в графе. В первую очередь изменения касаются поиска максимального пути при переходе от одной вершины графа к другой. Происходит поиск пути наиболее простого развития СИ-атаки

с точки зрения злоумышленника. На очередном шаге алгоритма, когда осуществляется переход к новому пользователю, поиск пользователя производится путем поиска максимальной общей вероятности успешности элементарных СИ-атакующих действий злоумышленника. Следующим отличием является то, что поиск осуществляется до того момента, как будет получен пользователь, свойства которого указывают на наличие требуемой злоумышленнику конфиденциальной информации. Если такой пользователь не найден, то считается, что данная конфиденциальная информация защищена от СИ-атак, направленных на пользователей информационных систем.

3. Пример программной реализации рассмотренного алгоритма. Внедрение данного алгоритма в разработанный ранее программный комплекс (его рассмотрению были посвящены статьи [1–3, 12–15]) позволило обеспечить автоматизацию одного из вариантов анализа защищенности пользователей информационных систем от СИ-атакующих действий злоумышленника. В данный момент реализовано текстовое представление итогов СИ-атаки. Данное меню представлено на Рис. 2.

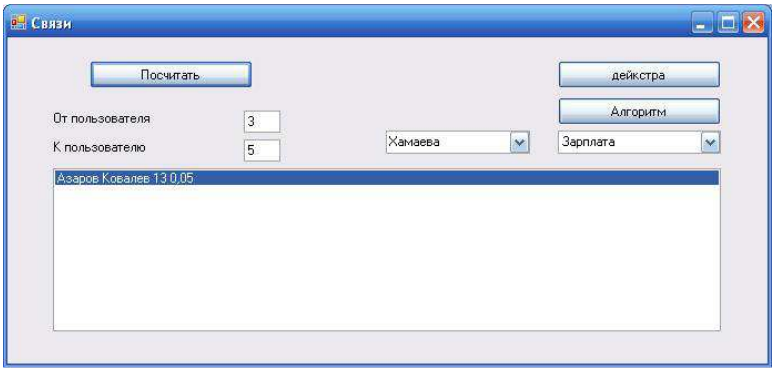

Рис. 1. Вывод результатов СИ-атаки на пользователей информационных систем.

Результат СИ-атаки находится в текстовом поле. Надпись «Азаров Ковалев 13 0,05» означает, что конфиденциальная информацию, требуемая злоумышленнику найдена. Злоумышленник получит доступ к данной информации с вероятностью 0,05. Первым звеном в СИ-атаке злоумышленника является пользователь с никнеймом «Азаров», информация была найдена на устройствах, доступных пользователю с никнеймом «Ковалев». В стадии реализации находится визуализация данной СИ-атаки с выводом всей цепочки связанных с злоумышленником пользователей с подробным описанием уязвимостей и степеня-

ми проявления этих уязвимостей для каждого пользователя информационной системы.

4. Заключение. В данной статье рассмотрены ключевые шаги алгоритма анализа резистентности пользователей от элементарных СИ-атакующих воздействий злоумышленника с применением профиля уязвимостей пользователя.

Предложенный подход представлен перечисленными принципиальными шагами алгоритма, который позволяет анализировать защищенность критичной информации от несанкционированных действий пользователя, находящегося под СИ-атакующим воздействием злоумышленника. В данном подходе учитывается степень выраженности уязвимостей пользователя, а также веса связей (вероятности успешного перехода) между пользователями.

Полученный программный продукт позволяет автоматизировать анализ защищенности пользователей информационных систем от СИ-атак с применением анализа степени выраженности уязвимостей пользователя, содержащихся в частичном профиле уязвимостей пользователя, построенном на психологических особенностях личности.

В то же время, данный программный продукт позволит получить временные оценки работы алгоритма, что позволит адаптировать его работу ради ускорения вычислений всего программного комплекса.

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. *Ванюшичева О.Ю.* Прототип комплекса программ для построения профиля психологически обусловленных уязвимостей пользователя. Диплоная работа. СПб.: СПбГУ, 2012.
4. *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.
5. *Котенко И.В., Юсупов Р.М.* Перспективные направления исследований в области компьютерной безопасности. Защита информации. Инсайд. 2006. № 2. С. 46.
6. *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.

7. *Петренко С.А.* Возможная методика построения системы информационной безопасности предприятия. // URL: http://bre.ru/security/13985.html (дата обращения 10.01.12)
8. *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.
9. *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.
10. *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.
11. *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.
12. *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.
13. *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.
14. *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.
15. *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.
16. *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.
17. *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.
18. *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.
19. *Фильченков А.А., Тулупьев А.Л.* Анализ циклов в минимальных графах смежности алгебраических байесовских сетей // Труды СПИИРАН. 2011. Вып. 2 (17). С. 151–173.

20. *Юсупов Р., Пальчун Б.П.* Безопасность компьютерной инфосферы систем критических приложений. Вооружение. Политика. Конверсия. 2003. № 2. С. 52.
21. *Dorothy D.E.* A Lattice Model of Secure Information Flow // Communications of the ACM. 2008. Vol. 19.No. 5. p. 236–243.
22. *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.
23. *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. IEEEComputerSociety, LosAlamitos. 2007. Washington. DC. USA. p. 1035-1042.
24. National Institute of Standards and Technology. URL: http://www.nist.gov/index.html (дата обращения 24.06.2012)
25. Siemens. The total information security toolkit. URL: http://www.cramm.com/(дата обращения 24.06.2012)
26. Software Engineering Institute. URL: http://www.cert.org/octave/ (датаобращения 24.06.2012)
27. *Toth T., Krugel C.* Evaluating the impact of automated intrusion response mechanisms //ACSAC 2002: Proceedings of the 18th Annual Computer Security Applications Conference. IEEEComputerSociety, LosAlamitos. 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 — 40. 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 — 40. 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.

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 15.01.2013.

РЕФЕРАТ

Азаров А.А. **Анализ защищенности пользователей информационных систем на основе графических моделей, содержащих профили уязвимостей.**

Проблема защиты критичной информации в настоящее время является одной из самых актуальных в информационных технологиях, хотя нельзя не признать, что, с исторической точки зрения, близкородственные ей проблемы зародились гораздо раньше — видимо, одновременно с возникновением письменности. Общепринятый подход к решению данных проблем заключается в развитии, диверсификации и усложнении применяемых технических мер обеспечения безопасности. Таким образом минимизируются возможности технических атак на системы. В то же время, каждая защищаемая информационная система имеет санкционированных пользователей, которые на законных основаниях работают в ней и зачастую имеют легальный доступ к конфиденциальной информации.

Целью данной статьи является построение алгоритма анализа резистентности пользователей информационных систем от социо-инженерных атак с учетом профиля уязвимостей пользователя.

Предложенный подход представлен перечисленными принципиальными шагами алгоритма, который позволяет анализировать защищенность критичной информации от несанкционированных действий пользователя, находящегося под СИ-атакующим воздействием злоумышленника. В данном подходе учитывается степень выраженности уязвимостей пользователя, а также веса связей (вероятности успешного перехода) между пользователями.

Полученный программный продукт позволяет автоматизировать анализ защищенности пользователей информационных систем от СИ-атак с применением анализа степени выраженности уязвимостей пользователя, содержащихся в частичном профиле уязвимостей пользователя, построенном на психологических особенностях личности.

В то же время, данный программный продукт позволит получить временные оценки работы алгоритма, что позволит адаптировать его работу ради ускорения вычислений всего программного комплекса.

SUMMARY

Azarov A.A. **Information systems' user's protection analysis on the basis of the graphic models containing user's vulnerabilities profile.**

The problem of critical information protection is now one of the most actual in information technologies though it is necessary to recognize that, from the historical point of view, closely related to its problems arose much earlier — probably, at the same time with writing emergence. The standard approach to the solution of these problems consists in development, diversification and complication of applied technical measures of safety. Thus possibilities of technical attacks to systems are minimized. At the same time, each protected information system has the authorized users who work at the lawful bases in it and often have legal access to confidential information.

The purpose of this article is creation of an analysis algorithm of resistance of users of information systems from socio-engineering attacks taking into account a profile of vulnerabilities of the user.

The offered approach is presented by the listed basic steps of algorithm which allows to analyze security of critical information from the unauthorized actions of the user being under SI-attacking of influences of the malefactor. In this approach degree of expressiveness of vulnerabilities of the user, and also weight of communications (probability of successful transition) between users is considered.

The received software product allows to automate the analysis of security of users of information systems from SI attacks with application of the analysis of degree of expressiveness of vulnerabilities of the user containing in a partial profile of vulnerabilities of the user, constructed on psychological features of the personality.

At the same time, this software product will allow to receive temporary evaluation of the work of algorithm that will allow to adapt its work for the sake of acceleration of calculations of all program complex.