УДК 614.8+002.6:004.89

А.Л. Тулупьев, А.Е. Пащенко, А.А. Азаров, Т.В. Тулупьева

ВИЗУАЛЬНЫЙ ИНСТРУМЕНТАРИЙ ДЛЯ ПОСТРОЕНИЯ ИНФОРМАЦИОННЫХ МОДЕЛЕЙ КОМПЛЕКСА «ИНФОМАЦИОННАЯ СИСТЕМА – ПЕРСОНАЛ», ИСПОЛЬЗУЮЩИХСЯ В ИМИТАЦИИ СОЦИОИНЖЕНЕРНЫХ АТАК

Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Тулупьева Т.В. **Визуальный инструментарий для построения информационных моделей комплекса «информационная система – персонал», использующихся в имитации социоинженерных атак.**

Аннотация. Описан прототип комплекса программ, с помощью которого продемонстрирована принципиальная возможность оценить защищенность персонала информационной системы от социоинженерных атак на основе обобщения подхода, ориентированного на анализ деревьев атак. Представление информационной системы и ее персонала в указанном комплексе программ опирается на иерархию информационных моделей, состоящую из информационной модели пользователя, информационной модели группы пользователей, информационной модели контролируемых зон, информационной модели программно-технического (программно-аппаратного) комплекса, информационной модели критичных информационных объектов (системы документов), информационной модели самой информационной системы, а также связей между соответствующими объектами. Приведен перечень использованных в разработке прототипа технологий, причины выбора этих технологий, а также краткое обоснование принятых проектных решений. Рассмотрен пример работы прототипа программного комплекса, как в ходе редактирования сведений об информационной системе и ее персонале, так и в ходе имитации социоинженерной атаки по рекомпенсационному типу на персонал этой системы.

Ключевые слова: информационная система, персонал, социоинженерная атака, визуальный редактор, злоумышленник.

Tulupyev A.L., Paschenko A.E., Azarov A.A., Tulupyeva T.V. **Visual toolkit for construction of the models of complex “information system – personnel”, used for imitation of socioengineering attacks.**

Abstract. The prototype of the program complex, used for demonstration of basic possibility for estimation the protection of personnel of informative system from socioengineering attack on the base of generalized approach, focused on analyze of trees of attacks, is described. The representation of informative system and its personnel in the specified program complex is based on hierarchy of information models, which consists of information model of the user, information model if the users group, information model of control area, information model of hardware and software complex, informative model of critical information objects (system of documents), information model of informative system itself and links between corresponded objects. The list of technologies, used during the development of this product, the reasons for using this technologies and brief substantiation of some technical solutions is resulted. The example of proceeding of program complex prototype during editing the information about socioengineering attack, as well as during the imitation of socioengineering attack on the recompensation type on the personnel of this system is considered.

Keywords: information system, personnel, socio-engineering attack, visual editor, malefactor.

1. Введение. В статьях [8–10], которые, в свою очередь, опирались на ряд более ранних работ [3–6, 12, 13, 15, 16], была сформирована иерархия информационных моделей для представления компонент комплекса «информационная система – персонал». Указанное представление позволяет описать сцену (контекст), в рамках которой могут развиваться социоинженерные атаки.

Цель настоящей работы — сформировать требования к функциональности комплекса программ, который позволяет имитировать социоинженерные атаки в рамках заданной сцены, а также привести пример работы прототипа такого комплекса (его функциональность ограничена одним видом атак — теми, которые имеют рекомпенсационный характер). Предполагается, что сам комплекс программ должен обеспечивать не только возможность создать новую сцену, отредактировать ее, сохранить или загрузить уже готовую, но и на основе перебора возможных атак (анализа дерева атак) сформировать оценку степени защищенности персонала системы. Кроме того, комплекс должен поддерживать имитацию возможных атак против заранее заданного пользователя. Также обсуждаются дальнейшие пути развития теоретических исследований и сопутствующих прикладных разработок.

2. Основные требования к комплексу программ. Комплекс программ должен включать следующие компоненты: базу данных, графический пользовательский интерфейс, библиотеку для создания и редактирования информационных систем, модуль для имитации социоинженерных атак.

База данных предназначена для хранения информационных моделей комплекса «информационная система – персонал»:

- информационная модель пользователя,
- информационная модель группы пользователей,
- информационная модель контролируемых зон,
- информационная модель программно-технического комплекса,
- информационная модель критичных информационных объектов (системы документов),
- информационная модель самой информационной системы.

Необходимые свойства указанных иных информационных моделей были описаны в статьях [9, 10]; перечень этих свойств задает, фактически, тот минимальный набор атрибутов, которыми должны обладать информационные модели. Логическая структура базы данных

представлена на рис. 1.

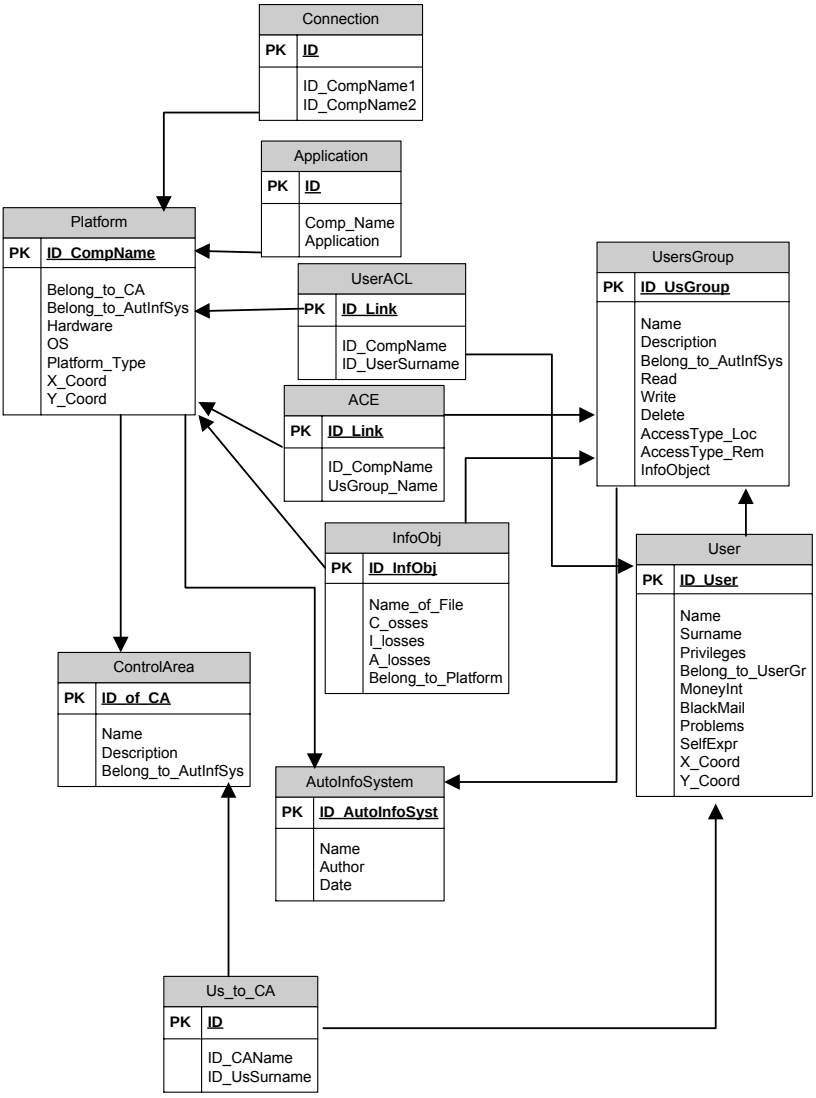

Рис. 1. Логическая схема базы данных.

Графический пользовательский интерфейс реализуется еще одной компонентой комплекса программ. Он предназначен, в первую очередь, для внесения данных в базу данных. Данные о каждой информационной модели вносятся отдельным интерфейсом (диалоговым окном), который позволяет ввести всю информацию об информационной модели. Кроме того, этот интерфейс позволяет графически отобразить информационную систему, а также редактировать сведения о ней, добавляя или удаляя составляющие системы, а также меняя свойства уже существующих объектов.

Графический пользовательский интерфейс дополняется компонентой комплекса программ, которая отвечает за визуализацию сцены (контекста), в которой может развиваться социоинженерная атака.

На данный момент реализована тестовая версия атаки, учитывающая возможность подкупа пользователя (т.е. атака по рекомпенсационному типу; другие атаки см. в [9]).

Для имитации реализации этой атаки нужно внести следующие сведения:

- описание ресурсов злоумышленника,
- описание пользователя, на которого совершается атака,
- критичный информационный объект, который необходим злоумышленнику

Комплекс программ позволяет пользователю выбрать эти три набора свойств и внести конкретные значения. Указанный комплекс позволяет совершить имитацию атаки как из текстового режима работы, так и из графического. В текущей версии прототипа разница состоит лишь в том, что в первом режиме есть возможность выбора из полного списка ресурсов, а в графическом — сразу должен быть произведен выбор пользователя информационной системы, на которого будет совершена атака.

3. Реализация прототипа комплекса программ. Прототип комплекса программ был написан на объектно-ориентированном языке программирования java с помощью IDE NetBeans 6.8. Исходя из требований, изложенных в предыдущем разделе, необходимо решить следующие задачи:

- обеспечить работу с графами в графическом режиме для представления и редактирования моделей информационной системы и ее персонала;
- работа с базами данных для хранения сведений о сформированных объектах в процессе диалога с оператором.

В ходе решения первой задачи, была выбрана свободно распро-

страняемая библиотека jgraph, которая позволяет отображать граф и его дуги с помощью объекта jPanel. Применение этой библиотеки позволило решить вопрос о динамическом редактировании информационной системы. Благодаря использованию JPopupMenu оператору удобно выбрать необходимые действия, через которые осуществляется редактирование графа.

Решение второй задачи по разработке прототипа комплекса программ ограничивалось в первую очередь тем, что необходимо выбрать СУБД, которая

- установлена практически на любом компьютере предполагаемого оператора,
- проста в использовании.

Этим двум требованиям, на наш взгляд, полностью удовлетворяет СУБД Microsoft Access. Access является базовой составляющей Microsoft Office, что означает присутствие этой СУБД на значительной части современных офисных компьютеров. Соответственно, работать с прототипом комплекса сможет большинство потенциальных операторов. Кроме того, существует инструментарий, позволяющий автоматически перейти (осуществить upscaling) с указанной СУБД на более сложные системы, например — на MS SQL Server.

Реализация взаимодействия java и MS Access также требует особого внимания. Java может обращаться к этой СУБД несколькими способами (речь идет о способах, доступных на основе свободно распространяемого ПО):

- jdbc-odbc bridge,
- pure ODBC,
- использование бесплатных библиотек.

Для разработки прототипа комплекса программ был выбран первый вариант, в силу его большей распространенности. Таким образом, удалось подключиться к БД и сохранять–загружать туда и оттуда информацию. Соответственно, информация, хранимая в БД, полностью определяется теми информационными моделями, которые обеспечивают построение представления информационной системы и ее персонала (см. [9, 10]). Для обеспечения удобства разработки комплекса программ, были сформированы классы, которые также полностью соответствуют указанным выше информационным моделям.

Исходя их поставленных задач, программный код был разделен на три логические составляющие: Model, View, Controller. В Model присутствуют те классы, которые соответствуют информационным моделям. В Controller — классы, отвечающие за основные операции, ис-

полняемые программой. View содержит набор классов, которые отвечают за визуальную составляющую программного продукта.

4. Пример работы визуального инструментария. На основе реализованного прототипа комплекса программ разбирается тестовый пример, который реализует модель информационной системы, состоящей из следующих элементов: 3 пользователей, 5 устройств, 1 контролируемой зоны, нескольких связей между пользователями и устройствами. Один из пользователей обладает правами администратора и доступом ко всем устройствам, другие же — правами «обычного пользователя». Визуальное представление модели такой информационной системы приведено на рис. 2 — этот результат получен в графическом режиме работы визуального инструментария.

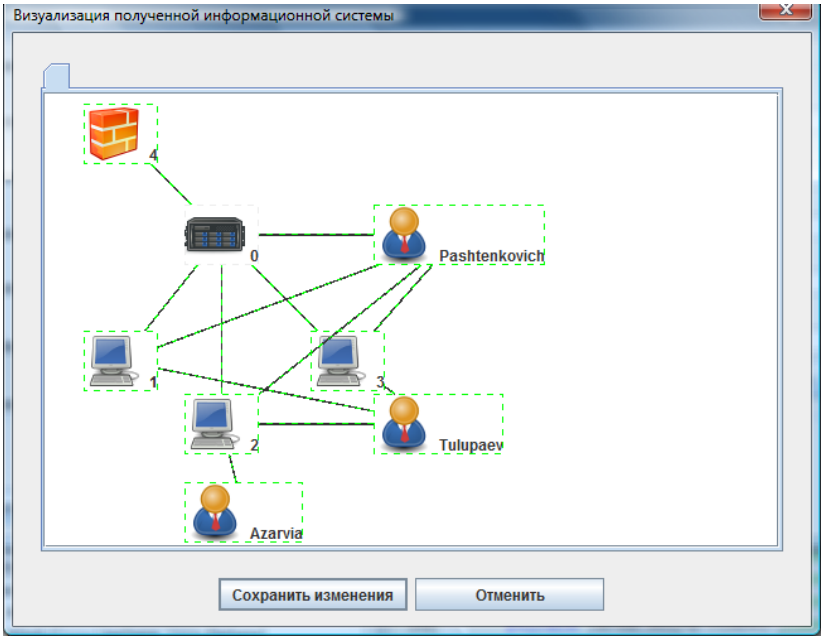

Рис. 2. Визуализация модели информационной системы.

Примером атаки может послужить атака по рекомпенсационному типу на пользователя Azarvia. На каждом устройстве хранятся определенные информационные объекты. Реализуется алгоритм имитации атаки, приведенный в статье [9], но с учетом того, что проверка до-

ступности информационных объектов изменена: через пользователя проверяется наличие объектов на тех устройствах, к которым у него есть доступ, и, в случае неудачи, обращается к другим пользователям, у которых, возможно, есть доступ к тем устройствам, к которым нет доступа у текущего пользователя. Таким образом, ход атаки будет проходить следующим образом (приводится фрагмент журнала имитируемых событий – атакующих действий):

- проверка возможности подкупа интеллектуального агента Azarvia;
- интеллектуального агента Azarvia подкупить удалось;
- проверяем наличие необходимой злоумышленнику информации на устройствах;
- на доступных интеллектуальному агенту Azarvia устройствах необходимой информации нет;
- интеллектуальный агент Azarvia начинает сканировать сеть;
- смотрит, к каким устройствам подключено то устройство, к которому у интеллектуального агента Azarvia есть доступ;
- смотрит, у каких интеллектуальных агентов есть доступ новым устройствам
- атака пойдет по интеллектуальному агенту Pashtenkovich;
- проверка возможности подкупа интеллектуального агента Pashtenkovich;
- интеллектуального агента Pashtenkovich подкупить удалось;
- проверяем наличие необходимой злоумышленнику информации на устройствах;
- информация найдена, атака успешна.

Полученный результат говорит о том, что атака на информационную систему завершилась, с точки зрения злоумышленника, успешно, а, значит, защита персонала системы от социоинженерных атак неудовлетворительна.

5. Уязвимость пользователя. Анализируя вышеописанную схему атаки, становится понятно, что злоумышленнику нужно располагать данными о возможных уязвимостях пользователя для того, чтобы атака прошла успешно. Соответственно, для повышения защиты информационной системы нужно выявить, учесть и ослабить уязвимости (уменьшить степень проявления или степень критичности уязвимостей) каждого ключевого пользователя, имеющего доступ к значимой (критичной) информации. В статье [8] были указаны группы сотрудников, способных намеренно (осознанно) реализовывать действия, направленные на нарушение безопасности информации. Руководству организации, если оно хочет повысить защиту информационной системы, целесообразно определить особенности уязвимости ключевых пользователей. Зная уязвимости, можно построить профилактическую работу (более широко — систему организационных и организационно-технических мероприятий) с ключевыми пользователями по правиль-

ному поведению при социоинженерных атаках.

Минимальный перечень действий, который потребуется для формирования реестра уязвимостей предполагает следующие шаги:

1. Выявить сотрудников, попавших в сложную жизненную ситуацию (болезнь, болезнь близких, сложные отношения в семье, потеря близкого человека). Такие сотрудники наиболее подвержены социоинженерным атакам из-за неустойчивого эмоционального состояния;

2. Выявить сотрудников, совершивших крупную покупку (квартира, машина, дача и т. п.). Такие сотрудники, если они испытывают материальные трудности, более восприимчивы к подкупу;

3. Выявить сотрудников, которые рассчитывали на повышение, вознаграждение, перевод в другой отдел, получение дополнительных льгот, но не получили их;

4. Определить личностные особенности сотрудников, повышающие уязвимость пользователя, с помощью психодиагностических методик. В настоящее время есть много сборников психодиагностических методик, например [7]. К таким личностным особенностям можно отнести: любопытство, доверчивость, демонстративность, стремление быть в центре внимания, низкий интеллект, неразвитое логическое мышление и т.п.;

5. Определить степень выраженности различных потребностей. В том числе, потребности во власти, в достижениях, в принадлежности. Для этого можно использовать, например, методику диагностики степени удовлетворения основных потребностей [7];

6. Определить уровень выраженности различных механизмов психологической защиты, модифицирующих поведение сотрудников. Интенсивно работающая психологическая защита, как бессознательный механизм регуляции поведения, не позволяет сотруднику адекватно оценить обстановку [2]. Высокое отрицание, например, может привести сотрудника к недоучету важных факторов воздействия или недопониманию важности имеющейся информации и неправильной оценке последствие совершенного поступка. Проекция поможет сотруднику освободиться от ответственности и ощущения вины за сделанное и переложить ответственность на кого-то другого. Рационализация позволит сотруднику найти ложные причины для оправдания своего поведения. Определение функционирования психологической защиты можно проводить при помощи методики «Индекс жизненного стиля» Келлермана–Плутчика [1] или методики М.Бонда [11].

Таким образом, выявление уязвимостей пользователей позволит отделу по работе с персоналом или отделу информационной безопас-

ности разработать систему профилактических мероприятий, позволяющих уменьшить вероятность успешности социоинженерных атак.

6. Направление дальнейших исследований. Особую значимость в контексте социоинженерных атак представляют топ-менеджеры и руководители высшего звена организации. Эти сотрудники обладают доступом к широкому спектру информации и, при условии успешности социоинженерной атаки, могут осознанно или неосознанно передать злоумышленнику информацию исключительной важности. В настоящее время согласно выводам, сделанным в [14], в большинстве российских компаний система вознаграждения топ-менеджмента не привязана к эффективности управления компанией. В подобной ситуации возникает проблема агентских издержек. Суть теории агентских издержек заключается в том, что агенты (управленцы), нанятые собственниками или акционерами, действуют так, чтобы максимизировать полезность для себя, а не для принципала (тех самых собственников или акционеров). Это происходит в ситуации, когда последствия экономических действий агентов ложатся на их плечи не полностью, существенная часть приходится на долю собственника или акционера, то есть агент делит риски своей деятельности. Как следствие, менеджер может поддаться на социоинженерные атаки (или в недостаточной степени предпринимать усилия по контролю своих действий, рискованных с точки зрения социоинженерных атак), чтобы максимизировать свою выгоду. В качестве факторов, повышающих уязвимость менеджеров, можно выделить отсутствие четкой стратегии корпоративного развития компании; отсутствие прямой экономической заинтересованности менеджеров в повышении рыночной капитализации; неудовлетворительное качество раскрытия информации о деятельности компании; недостаточная степень прозрачности финансовых потоков компании [14].

С одной стороны, указанные уязвимости требуют разработки подходящих моделей для их учета в оценке степени защищенности персонала информационных систем от социоинженерных атак. С другой стороны, очевидны первые шаги, такие как повышение качества корпоративного управления, введение опционных планов для руководства [14], которые могут быть предложены в качестве мер по снижению уровня соответствующих рисков. Однако это можно рассматривать только как начальный этап — оценка эффективности указанных мер может быть выполнена только при наличии развитой системы методов, моделей и алгоритмов упомянутой оценки степени защищенности персонала информационных систем от социоинженерных атак. Данная

проблема потребует дальнейшего рассмотрения.

7. Заключение. Разработан прототип комплекса программ, с помощью которого продемонстрирована принципиальная возможность оценить защищенность персонала информационной системы от социоинженерных атак на основе обобщения подхода [6, 15, 16], ориентированного на анализ деревьев атак.

Представление информационной системы и ее персонала в указанном комплексе программ опирается на иерархию информационных моделей, состоящую из информационной модели пользователя, информационной модели группы пользователей, информационной модели контролируемых зон, информационной модели программно-технического (программно-аппаратного) комплекса, информационной модели критичных информационных объектов (системы документов), информационной модели самой информационной системы, а также связей между соответствующими объектами, рассмотренных в статьях [8-10].

Функциональность прототипа в построения деревьев атак ограничена: имитируются социоинжинерные атаки рекомпенсационного типа.

Кратко рассмотрены пути дальнейшего развития теоретических исследований и прототипа комплекса программ.

Литература

1. *Вассерман Л.И.* (под ред.). Психологическая диагностика индекса жизненного стиля. (Пособие для врачей и психологов) / СПб., 1998. 48 с.
2. *Грановская Р.М.* Психологическая защита. СПб.: Речь, 2010. 476 с.
3. *Котенко И. В., Степашкин М. В., Богданов В. С.* Анализ защищенности компьютерных сетей на этапах проектирования и эксплуатации // Изв. вузов. Приборостроение. 2006. Т. 49, № 5. С. 3–8.
4. *Котенко И. В., Степашкин М. В., Богданов В. С.* Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 7–24.
5. *Котенко И. В., Степашкин М. В.* Использование ложных информационных систем для защиты информационных ресурсов компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2005. № 1. С. 63–73.
6. *Котенко И. В., Степашкин М. В.* Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Изв. вузов. Приборостроение. 2006. Т. 49, № 3. С. 3–8.
7. *Райгородский Д.Я.* (редактор-составитель). Практическая психодиагностика. Методики и тесты. Учебное пособие. Самара: Издательский Дом «БАХРАХ-М», 2001. 672 с.
8. *Тулупьева Т.В., Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Степашкин М.В.* Социально-психологические факторы, влияющие на степень уязвимости пользователей

информационных систем, с точки зрения социоинженерных атак // Труды СПИИРАН. 2010. Вып. 1(12).[в печати]
9. *Тулупьев А.Л., Пащенко А.Е., Азаров А.А.* Информационная модель пользователя, находящегося под угрозой социоинженерной атаки // Труды СПИИРАН. 2010. Вып. 2(12).[в печати]
10. *Тулупьев А.Л., Пащенко А.Е., АзаровА.А.* Информационные модели компонент комплекса «информационная система – персонал», находящегося под угрозой социоинженерных атак. // Труды СПИИРАН. 2010. Вып. 1(13).[в печати]
11. *Туник Е.Е.* Психологические защиты. Тестовая методика. СПб.: Речь, 2010. 219 с.
12. *Фролова А. Н., Тулупьева Т. В., Пащенко А. Е., Тулупьев А. Л.* Возможный подход к анализу защищенности информационных систем от социоинженерных атак // Информационная безопасность регионов России (ИБРР-2007). V Санкт-Петербургская региональная конференция. Санкт-Петербург, 23–25 октября 2007 г.: Труды конференции / СПОИСУ. СПб., 2008. С. 195–199.
13. *Фролова А. Н., Пащенко А. Е., Тулупьева Т. В., Тулупьев А. Л.* Анализ уровня защищенности информационных систем в контексте социоинженерных атак: постановка проблемы // Труды СПИИРАН. 2008. Вып. 7. СПб.: Наука, 2008. С. 170–176.
14. *Ялов А. Н.* Ключевые проблемы недооцененности российских компаний // Российский экономический Интернет-журнал [Электронный ресурс]: Интернет-журнал АТиСО / Акад. труда и социал. Отношений. Электрон. журн. М.: АТиСО, 2008. № гос. регистрации 0420600008. http://www.e-rej.ru/Articles/2008/Yalov.pdf.
15. *Kotenko I.V., Stepashkin M.V.* Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life // Springer-Verlag Lecture Notes in Computer Science. 2005. Vol. 3685. P. 311–324.
16. *Kotenko I.V., Stepashkin M.V.* Network Security Evaluation Based on Simulation of Malefactor's Behavior // Proc. of the Intern. Conf. on Security and Cryptography (SECRYPT–2006), Setubal, 2006. P. 339–344.

Тулупьев Александр Львович — д.ф.-м.н., доцент; заведующий лабораторией теоретических и междисциплинарных проблем информатики (ТиМПИ) Учреждения Российской академии наук Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН), профессор кафедры информатики математико-механического факультета С.-Петербургского государственного университета (СПбГУ). Область научных интересов: представление и обработка данных и знаний с неопределенностью, применение методов математики и информатики в социокультурных исследованиях, применение методов биостатистики и математического моделирования в эпидемиологии, технология разработки программных комплексов с СУБД. Число научных публикаций — 210. 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 — PhD in Appl. Math. and CS, Dr. Sci. in CS, associate professor; head of laboratory, Theoretical and Interdisciplinary Computer Science Дфицкфещкн (TICS Lab), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), professor, Computer Science Department, Faculty of Mathematics and Mechanics, St. Petersburg State University (SPbSU). Research interests: uncertain knowledge and data representation and processing, application of mathematics and computer science in sociocultural studies, applications of biostatistics and mathematical modeling in modern epidemiology, software technologies and development of information systems with databases. The number of publications — 210. ALT@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14-th

Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Пащенко Антон Евгеньевич — младший научный сотрудник научно-исследовательской группы междисциплинарных проблем информатики Учреждения Российской академии наук С.-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: математическая статистика, статистическое моделирование, применение методов биостатистики и математического моделирования в эпидемиологии. Число научных публикаций — 35. AEP@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.

Paschenko Anton Evgen'evich — junior researcher, Interdisciplinary Computer Science Research and Development Group, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: mathematical statistics, statistical modeling, application of biostatistics and mathematical modeling in epidemiology. The number of publications — 35. AEP@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Азаров Артур Александрович — студент Санкт-Петербургского Государственного Университета Математико-Механического и Экономического факультетов. Область научных интересов: автоматизация анализа защищенности информационных систем с учетом социоинженерных атак. Число научных публикаций — 2. 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 — student of Saint-Petersburg State University of the faculties of Mathematics and Mechanics and Economics. Research interests: the analyzing protection of informative systems concerning socioengineering's attacks. The number of publications — 2. artur-azarov@yandex.ru, www.tulupyev.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Тулупьева Татьяна Валентиновна — к.психол.н., доцент; старший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики (ТиМПИ) Учреждения Российской академии наук С.-Петербургский институт информатики и автоматизации РАН (СПИИРАН), доцент кафедры информатики математико-механического факультета С.-Петербургского государственного университета (СПбГУ), доцент кафедры психологии управления и педагогики Северо-Западной академии государственной службы (СЗАГС). 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 — около 70. 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 — PhD in Psychology, associate professor; senior researcher, Theoretical and Interdisciplinary Computer Science Laboratory (TICS Lab), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), associate professor, Computer Science Department, Faculty of Mathematics and Mechanics, St. Petersburg State University (SPbSU), associate professor, Management Psychology and Pedagogic Department, North-West Academy of Public Administration

(NWAPA). 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 — 70. TVT@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Поддержка исследований. Настоящая работа частично поддержана грантом РФФИ (проект № 10-01-00640-а) и грантом СПбГУ (Мероприятие 2, 2011–2013 гг.).

РЕФЕРАТ

Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Тулупьева Т.В. **Визуальный инструментарий для построения информационных моделей комплекса «информационная система – персонал», использующихся в имитации социо-инженерных атак.**

Разработан прототип комплекса программ, с помощью которого продемонстрирована принципиальная возможность оценить защищенность персонала информационной системы от социо-инженерных атак на основе обобщения подхода, ориентированного на анализ деревьев атак.

Представление информационной системы и ее персонала в указанном комплексе программ опирается на иерархию информационных моделей, состоящую из информационной модели пользователя, информационной модели группы пользователей, информационной модели контролируемых зон, информационной модели программно-технического (программно-аппаратного) комплекса, информационной модели критичных информационных объектов (системы документов), информационной модели самой информационной системы, а также связей между соответствующими объектами.

С помощью указанного прототипа, можно построить новую или отредактировать уже имеющуюся информационную систему и сохранить ее в удобном для пользователя виде. Имеется возможность, как текстового редактирования системы, так и визуального. В то же время, функциональность прототипа в построения деревьев атак ограничена: имитируются социо-инженерные атаки рекомпенсационного типа. Имитацию этой социо-инженерной атаки также можно провести, как из текстового, так и из визуального режима работы прототипа. Рассмотрена только эта социо-инженерная атака в силу того, что вероятность подобного события достаточно высока, и этот тип социо-инженерной атаки необходимо обработать в первую очередь.

Кратко рассмотрены пути дальнейшего развития теоретических исследований и прототипа комплекса программ. Предполагается, что для повышения уровня защиты информационной системы нужно выявить, учесть и ослабить уязвимости (уменьшить степень проявления или степень критичности уязвимостей) каждого ключевого пользователя, имеющего доступ к значимой (критичной) информации. Кроме того, при развитии предпринятого подхода к анализу защищенности представляется целесообразным воспользоваться результатами экономической теории агентских издержек.

SUMMARY

Tulupyev A.L., Paschenko A.E., Azarov A.A., Tulupyeva T.V. **Information models of the components of complex "Informative system – personnel", which is under threat of socioengineering attack.**

The prototype of program complex, through which basic possibility of estimation protection of personnel of information system from socio-engineering attack on the base of generalized approach, oriented on the trees of attacks analyze, has been demonstrated, was developed.

Representation of information system and its personnel in the specified program complex is based on hierarchy of information models, which consists of information model of the user, information model if the users group, information model of control area, information model of hardware and software complex, informative model of critical information objects (system of documents), information model of informative system itself and links between corresponded objects.

With the help of specified prototype it is able to build new or edit already available information system and save it with convenient for user method. There is a possibility to edit system both in text and graphics modes. At the same time, functionality of prototype in building trees of attack is limited as it can imitate only socio-engineering attacks of recompensation type. Imitation of this attack is also available to create both trough text and graphics modes. Current socio-engineering attack is considered as the possibility of this event is quite high and this type of socio-engineering attack should be estimated in the first rate.

Further development of theoretical issues and development of program prototype is briefly considered in this article. It is supposed that for increase the protection level of informative system, it is essential to reveal, consider and weaken vulnerability (reduce the rate of displays or rate of critical level of vulnerabilities) of each key user, who has the access to valuable (critical) information. What is more, during the development of used approach to analyzing of protection it is represented expedient to use the theory of economic theory of agents costs.