УДК 614.8 + 002.6:004.89

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

ПРОТОТИП КОМПЛЕКСА ПРОГРАММ ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ПЕРСОНАЛА ИНФОРМАЦИОННЫХ СИСТЕМ, ПОСТРОЕННЫЙ НА ОСНОВЕ ФРАГМЕНТА ПРОФИЛЯ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЯ

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.**

Аннотация. Комплексные корпоративные информационные системы в настоящее время получают все большее распространение в современном мире. Разработка, поддержка и защита подобных систем занимает значительное количество времени и ресурсов, кроме того только высококвалифицированные специалисты могут заниматься подобными системами. Информация, хранимая в таких информационных системах, имеет огромную ценность для компаний-владельцев систем, поэтому значительные усилия затрачиваются на построение системы защиты таких систем от различных угроз безопасности. Целью данной статьи является комбинация нечеткого и вероятностного подхода к оценке защищенности пользователя по отношению к атакующим действиям злоумышленника, причем рассматриваются действия достаточно элементарного характера («одноходовки»), нацеленные на «элементарные» уязвимости пользователя, воздействие на которые приводит непосредственно к какому-то действию пользователя.

Ключевые слова: социо-инженерная атака, информационная система, пользователь, профиль уязвимостей пользователя.

Azarov A.A., Tulupyeva T.V., Tulupyev A.L. **Software prototype for information systems' personnel's protection analysis based on the fragment of user's vulnerabilities profile.**

Abstract. Complex corporate information systems are widely distributed in the modern world. Development, support and protection of similar systems require a significant amount of time and resources, besides only highly skilled experts can be engaged in the management of such systems. Information stored in such information systems has enormous value for the owners of systems therefore considerable efforts are spent for creation systems of protection of such systems from various threats to their safety. The purpose of this paper is to combine an indistinct and likelihood approach to an assessment of security of the user in relation to attacking actions of the malefactor, meaning the actions of rather elementary character ("one movement") aimed at "elementary" vulnerabilities of the user which lead directly to some action of the user.

Keywords: socio-engineering attack, informational system, user, user's vulnerabilities profile.

1. Введение. Переход современной общественной формации от индустриального к информационному обществу обуславливает широкое распространение информационных систем, которые становятся корпоративными ценностями наряду с денежными средствами, ценными бумагами и ресурсами компании [22–25]. Информация, хранимая в таких информационных системах, имеет огромную ценность для

компаний-владельцев систем, поэтому значительные усилия затрачиваются на построение системы защиты таких систем от различных угроз безопасности. Новейшие системы безопасности могут защитить информационные системы от большинства программно-технических атак, а также серьезно осложнить жизнь злоумышленникам, пытающимся добраться до конфиденциальной информации, но в то же время большинство таких систем не защищено от внутренних угроз, исходящих от пользователей таких систем [5, 6, 11, 12]. Таким образом, злоумышленники, обладающие навыками социо-инженеров, могут с легкостью завладеть столь ценной конфиденциальной информацией лишь совершив атакующие воздействия на уязвимости пользователей информационных систем.

Необходимо научиться защищать информацию от такого типа атак (т.е. социо-инженерных атак или социотехнических атак). Кроме того необходимо научиться оценивать уровень защищенности персонала информационных систем от социо-инженерных атак. То есть, поскольку подобные атаки используют пользователей информационных систем в качестве основного пути развития атаки, необходимо научиться прогнозировать уязвимости пользователей информационных систем, а также строить агрегированные, сводные показатели защищенности или уязвимости персонала «в целом».

Подобные показатели могут служить индикаторами того, насколько пользователи подвержены тому или иному действию злоумышленника (атакующему действию в простейшем случае; атаке — серии атакующий действий — в более общем случае; набору атак, которые вообще может предпринять злоумышленник при заданной квалификации и доступных ресурсах — в самом общем случае). Также можно предположить, какие действия будут совершены пользователем в ответ на действия злоумышленника и с какой вероятностью. Наконец, зная вероятность успеха реализации атаки и уровень критичности информационного ресурса (например, электронного документа), можно оценить ожидаемый ущерб.

При этом необходимо сделать важную оговорку: критичность информационных ресурсов может быть выражена как количественно, и тогда оценка ожидаемого ущерба сведется к построению математических ожиданий и иных характеристик особых случайных величин, так и с помощью порядковой шкалы (например, «некритичен – малокритичен – критичен – очень критичен – исключительно критичен – особо важен», то есть, Лайкерт-шкалы), и тогда оценивать ожидаемый ущерб придется с помощью комбинирования вероятностного и нечеткостного

подходов. Наконец, в силу того, что ряд оценок критичности информационного ресурса и вероятности успеха реализации атакующего действия, а также вероятности ответного действия пользователя будут задавать эксперты, стоит ожидать, что поступающая от них информация будет обладать нечеткостью или иными видами неточности, неполноты, несовершенства, что делает неизбежным применение гибридных моделей при агрегации имеющихся сведений и построения сводных показателей для оценки степени защищенности персонала информационной системы от социо-инженерных атак.

Целью данной статьи является формирование на основе комбинации нечеткого и вероятностного подхода принципа построения оценки защищенности пользователя по отношению к атакующим действиям злоумышленника, причем в силу ограничений экспериментальной базы — результатов соответствующего пилотного исследования[7] — рассматриваются действия достаточно элементарного характера («одноходовки»), нацеленные на «элементарные» уязвимости пользователя, воздействие на которые приводит непосредственно к какому-то действию пользователя.

2. Построение фрагмента профиля уязвимостей пользователя. Теоретическое объяснение классификации уязвимостей [1–4, 7, 13-16] не дает ответа на вопрос, как их выявлять, вычислять и прогнозировать. Чтобы выразить уязвимости через психологические характеристики личности, необходимо придумать алгоритм, при помощи которого можно будет переводить психологические особенности пользователя в уязвимости. С этой целью было проведено социологическое исследование, основной задачей которого был поиск взаимосвязи между психологическими особенностями, действиями пользователя и определением уязвимостей пользователя. Данное исследование предполагало создание анкеты, основанной на экспертном анализе прогнозируемых уязвимостей пользователя, обработку данных анкет с помощью статистического пакета SPSS и выявление уязвимостей пользователя, согласно полученным данным.

Исследование носило пилотный характер, и следует отметить, что при интерпретации результатов возможны погрешности. В исследовании принимали участие студенты двух вузов Санкт-Петербурга. Всего отвечало на вопросы анкеты 84 человека. Возраст респондентов составлял 17–24 года. Подавляющее большинство студентов учится на гуманитарных факультетах. Респондентам предлагалось ответить на 43 вопроса анкеты. Полученные данные обрабатывались на программе SPSS.

Владея эмпирическими данными по совместному проявлению психологических особенностей и склонности, выявленной, фактически, с помощью проективной методики, к тем или иным действиям, увязанным с потенциальными уязвимостями, можно использовать известные статистические методы для построения (или, скорее, прогнозирования) профиля уязвимостей пользователя через его профиль психологических особенностей.

Интерпретация результатов производится следующим образом: фактор определяется теми переменными (вопросами), значения коэффициентов которых больше 0,3. Таким образом, были получены определяющие вопросы для каждого из факторов. Поэтому из вопросов было выделено 5 факторов. Однако, для того чтобы убедиться, что эти факторы и есть уязвимости пользователей, необходимо провести корреляционный анализ. Для этого полученные факторы были представлены в численном виде.

Таким образом, было получено пять уязвимостей пользователя:

1) техническая неосмотрительность (пользователь имеет низкую самооценку по внешности, низкая потребность в новых ощущениях, низкий уровень средней самооценки);

2) слабый пароль (пользователь склонен к безалаберности, невнимательности, в том числе и по отношению к безопасности своих идентификационных данных. У него высокий уровень подозрительности, он очень самоуверен. Вместе с тем у него плохая слуховая память, и он ярко выраженный меланхолик);

3) техническая халатность и установка на получение личной выгоды (пользователь подозрителен, у него высокая самооценка по авторитету у сверстников, он дипломатичен, не склонен переживать из-за каких-либо проблем. Вместе с тем он ставит перед собой нереальные цели в умении делать многое своими руками и наоборот очень скромно оценивает свои возможности, у него низкая склонность к риску, он не мстителен и недооценивает свои умственные возможности);

4) техническая неопытность (пользователь обладает высоким вытеснением и рационализацией, то есть он невнимателен, излишне самоуверен, склонен переоценивать свою значимость и игнорировать проблемы. Он сдержан в проявлении своих чувств, практичен и рассудителен, отличается радикализмом, то есть любит экспериментировать, открыт для чего-то нового, несклонен к бескомпромиссности и у него высокий психологический возраст);

5) техническая безграмотность (пользователь склонен срывать свою злость на других, у него высокий уровень интеллекта, он эмоци-

онально нестабилен, все время находится в расслабленном состоянии, стремится контролировать любую значимую ситуацию, считает, что его успехи обусловлены внешними обстоятельствами – удачей, везением. Такой человек не склонен считать себя ответственным за свои неуспехи и неудачи, он приписывает эту ответственность другим людям, также такой человек считает, что он легко завоевывает уважение других людей).

В зависимости от того, на какую из этих уязвимостей пользователя злоумышленник направляет свое атакующее воздействие, можно выделить различные варианты атакующих воздействий и ответные действия пользователя на них.

Было рассмотрено несколько возможных, но не исчерпывающих вариантов атакующих воздействий и ответов на них. Все они представлены в таблице ниже.

Таблица 1. **Атакующие воздействия и ответы пользователя на них**

Уязвимость	Атакующее воздействие	Действие пользователя
Техническая неосмотрительность	Предложение зарегистрироваться на каком-то привлекательном сайте	Пользователь регистрируется, вводя старые идентификационные данные
	Отправка письма с «полезным» для пользователя приложением	Пользователь читает письмо и устанавливает присланное приложение
	Виртуальное знакомство с пользователем в сети	Под действием обаяния злоумышленника пользователь выдает свои идентификационные данные
Слабый пароль	Взломать	-
	Подсмотреть	-
Техническая халатность и установка на получение личной выгоды	Подкуп	Передача злоумышленнику идентификационных данных за услугу
	Предложение зарегистрироваться на каком-то привлекательном сайте	Пользователь регистрируется, вводя старые идентификационные данные
Техническая неопытность	Предложение зарегистрироваться на каком-то привлекательном сайте	Пользователь регистрируется, вводя старые идентификационные данные
	Отправка письма с «полезным» для пользователя приложением	Пользователь читает письмо и устанавливает присланное приложение
	Виртуальное знакомство с	Под действием обаяния

	пользователем в сети	злоумышленника пользователь выдает свои идентификационные данные
Техническая безграмотность	Предложение зарегистрироваться на каком-то привлекательном сайте	Пользователь регистрируется, вводя старые идентификационные данные
	Отправка письма с «полезным» для пользователя приложением	Пользователь читает письмо и устанавливает присланное приложение
	Предложение помощи в решении компьютерных дел	Принять помощь

Рассмотрим подробнее каждую из этих ситуаций. Если злоумышленник решил направить свое атакующее воздействие на уязвимость «Техническая неосмотрительность», то он может воспользоваться одним из видов вышеописанных воздействий. Так как пользователь является активным участником виртуальной среды, у него высокая широта социальных связей. Как правило, такие люди зарегистрированы в различных социальных сетях, ведут свои блоги или пишут в twitter. Если злоумышленник примет данный факт во внимание, он может, например, в той же социальной сети выслать пользователю приглашение зарегистрироваться на каком-то похожем сайте (социальная сеть, живой журнал и т.д.). Естественно, такой сайт будет подставным и так как у пользователя в той или иной степени проявляется уязвимость «информационная неосмотрительность», он соответственно с той или иной степенью может зарегистрироваться на подставном сайте, используя старые идентификационные данные, которые без труда узнает злоумышленник. Или же, последний сможет отправить пользователю письмо на электронную почту с каким-то интересным для данного пользователя приложением (например, программа для просмотра переписки своих друзей с третьими лицами). Пользователь в зависимости от степени проявления своей уязвимости установит данное приложение с той или иной вероятностью. И, наконец, опять же ввиду того, что пользователь является очень активным виртуальным собеседником, злоумышленник может с ним познакомиться в виртуальной среде и, тем или иным способом используя свое обаяние или другие качества, с той или иной степенью вероятности выяснить идентификационные данные пользователя.

Когда злоумышленник направляет свое атакующее воздействие на уязвимость «Слабый пароль», он не взаимодействует непосредственно с самим пользователем. То есть пользователь на исход социо-

инженерной атаки никаким образом повлиять не сможет. Более того, он даже не узнает, что она состоялась и его идентификационными данными обладает другой человек. В данном случае, если злоумышленник взламывает пароль пользователя, то вероятность получения этого пароля будет зависеть только от его сложности и места, где он находится. Если же злоумышленник использует атакующее воздействие «подсмотр пароля», то тут пользователь также может не понять, что произошло, и успешный исход социо-инженерной атаки зависит от сложности пароля и поведения злоумышленника.

«Техническая халатность и установка на получение личной выгоды» — уязвимость, сочетающая в себе две отличительные характеристики пользователя. С одной стороны, он небрежно относится к своим идентификационным данным, с другой – нацелен на получение личной выгоды. Злоумышленник может принять каждую из этих сторон (или одновременно обе) во внимание и выполнить вышеперечисленные атакующие воздействия. Если злоумышленник решил воздействовать на стремление пользователя получить личную выгоду, то он может либо подкупить его деньгами, либо получить идентификационные данные, оказав пользователю какую-либо услугу.

Часто одной из проблем современных сотрудников фирмы является их компьютерная безграмотность. Для решения той или иной компьютерной проблемы (завис компьютер, не печатает принтер и др.) на работе они обращаются за помощью к системному администратору. Но как быть пользователю, если последнего нет на месте или, например, пользователь работает дома в удаленном режиме? Злоумышленник может воспользоваться такой ситуацией и предложить пользователю свою помощь, а так как у пользователя присутствует уязвимость «Техническая безграмотность», он с той или иной вероятностью предоставит доступ к своему компьютеру, при чем сам при этом может даже удалиться, например, на кухню заваривать чай для хорошего «помощника».

Из всего вышеперечисленного очевидно, что определенное влияние злоумышленника на пользователя приводит к активации сразу нескольких уязвимостей. Так, например, действие злоумышленника "Отправка письма с «полезным» для пользователя приложением" активирует уязвимости техническая неосмотрительность, техническая неопытность и техническая безграмотность. Степень проявления каждой из этих уязвимостей переводится в вероятность на основании значений соответствующей уязвимости. Соответствующие вероятности для уяз-

вимостей обозначены p_1, p_2, p_3. Таким образом, при ряде предположений общая вероятность будет вычисляться по формуле

$$p(x) = 1 - (1 - p_1)(1 - p_2)(1 - p_3).$$

Таким же образом рассчитываются вероятности реакции пользователя на действия «предложение зарегистрироваться на каком-то привлекательном сайте» и «виртуальное знакомство с пользователем в сети».

Кроме того, очевидным образом из всех действий злоумышленника выделяются два итоговых состояния, в которые может прийти злоумышленник. Он может получить идентификационные данные пользователя, или же он получит доступ к компьютеру пользователя. Соответствующие общие вероятности также получаются с помощью формулы того же типа, что и формула представленная выше.

3. Модель комплекса «Информационная система – персонал – критичные документы» (комплекс ИСПКД). Для того чтобы приступить к оценке защищенности информационных систем необходимо в первую очередь формализовать модель указанного данного комплекса, причем следует принять во внимание, что при ее декомпозиции выделяется целый набор подмоделей — то есть моделей подсистем и персонала как одной из таких подсистем. С точки зрения имитации развития социо-инженерных атак, комплекс ИСПКД, а также злоумышленника удобно представлять в виде совокупности информационных моделей [1–8, 10, 11, 12].

Для представления информационной систем, персонала этой системы, а также связей между элементами системы и пользователями, выделяется ряд информационных моделей. Информационная система как модель IS {informational_system}, в которую включены ее общие свойства: когда и кем создана, название данной системы. Аппаратно-техническая составляющая информационной системы это двойка COMP {computers, links}, где computers включает в себя, какие именно устройства содержатся в данной системе, какое программное обеспечение на них установлено, в то время как links отображает прохождение связей между различными устройствами системы. Контролируемые зоны системы - это модель CA {control_area}. Данная модель была создана с целью разграничения зон доступа к аппаратно-технической составляющей системы. Подобные зоны, как правило, совпадают и с контролируемыми зонами предприятия в целом. Примером может служить кабинет директора. Без особого распоряжения туда никто, кроме директора, входить не может. Другой пример — серверная, в нее нет доступа ни у кого, кроме системных администраторов. Следу-

ющим элементом информационной системы является набор критических документов. Каждый набор документов это двойка DOC {location, value}, где location это привязка объекта к определенному устройству или придание ему общесетевого статуса, а value — оценка критичности документа.

В настоящей работе мы используем шкалу критичности документов от 0 (не критично) до 100 (чрезвычайно критично, особой важности). В данном случае считается сумма ущерба, который может быть нанесен компании, в случае если тот или иной документ станет доступен злоумышленнику. В дальнейшем планируется перейти к Лайкерт-шкале. Она состоит из «Некритичен – мало критичен – критичен в средней степени – очень критичен – особо важен». Но в таком случае сразу встает вопрос о применении гибридного подхода — необходимо комбинировать вероятностные оценки успешной реализации атаки и нечеткие оценки критичности финальных объектов атаки — критичных документов.

Следующей группой информационных моделей являются модели пользователей и групп пользователей. Модель пользователей US это тройка {id, general_inforamation, list_of_vulnerabilities}, где general_information включает в себя различные формальные атрибуты пользователей, такие как: ФИО, должность. List_of_vulnerabilities — это фрагмент профиля уязвимостей пользователя, состоящий из уязвимостей, которые приведены выше. Модель групп пользователей US_GR это двойка {user's_profiles, user's_access}, где user's_profiles-это права пользователей на совершение тех или иных действий, а user's_access — уровень доступа пользователей к различным аппаратно-техническим составляющим информационной системы.

Граф-носитель модели «Информационная система – персонал – критичные документы» допускает визуализацию [2, 3, 7, 10].

4. Оценка ущерба, наносимого социо-инженерными атаками. Формирование профиля уязвимостей позволяет формализовать модель пользователя и непосредственно приступить к анализу защищенности персонала информационных систем.

Перспективным подходом к подобному анализу является широко распространенный формализм — деревья атак[10]. Этот подход успешно применяется к анализу защищенности аппаратно-технической составляющей системы. Алгоритм работает по следующему принципу: каждое устройство COMP представляет собой хост, содержащий набор критичной информации DOC. Существенным допущением в данной модели является то, что рассчитывается критич-

ность хостов в целом, а не отдельных документов на данном хосте. Злоумышленник осуществляет ряд элементарных атакующих действий на COMP.computer, используя ошибки в программном и аппаратном обеспечении. После этого стоится дерево, каждый из листов которого — это успешно реализованное элементарное атакующее действие. Злоумышленник в каждом листе переходит в новое состояние, в зависимости от того какое именно элементарное атакующее действие было совершено. Соответственно он может продолжить развитие атаки на последующие хосты системы или же, если необходимая злоумышленнику информация найдена, завершить атаку. Соответственно подобный подход позволяет проанализировать защищенность информационной системы, но только аппаратно-технической составляющей информационной систем. Таким образом, без внимания остаются пользователи информационных систем, в то время как последние исследования показывают, что до 45% ущерба, наносимого компаниям из-за нарушения конфиденциальности информации, приходится именно на пользователей информационных систем и их умышленные или неумышленные противоправные действия.

В рассматриваемом программном комплексе данный подход модифицирован путем включения в рассмотрение пользователей информационных систем через построение информационной модели пользователя US и модели групп пользователей US_GR [17-20]. Основой такой модели стал разработанный US.user's_access.

Анализ защищенности информационной системы вместе с пользователями подразумевает построение более «глубокого» дерева атак. Это достигается за счет того, что добавляются элементарные атакующие воздействия злоумышленника, влияющие на US.user's_access. При влиянии на уязвимости происходят ответные действия пользователя. При имитации элементарных атакующих действий могут активироваться сразу несколько US.user's_access. В данной ситуации удобно использовать вероятностный подход к анализу защищенности пользователя. Таким образом, необходимо найти общую вероятность ответного действия пользователя на атакующее действие злоумышленника, влияющее на несколько уязвимостей, то есть надо найти $p(US.User's\_Access(\overline{1..n})$, где n — это число уязвимостей, на которые происходит влияние.

Примером такого действия может быть действие злоумышленника «Отправка письма с «полезным» для пользователя приложением», которое активирует уязвимости техническая неосмотрительность, техни-

ческая неопытность и техническая безграмотность. Каждая US.User's_access (i) с помощью специальной шкалы переводится в вероятность p_i. Для данного примера соответствующие вероятности для уязвимостей обозначены p_1, p_2, p_3. Оценки указанных вероятностей указывались с помощью экспертов. Каждое действие злоумышленника ведет к разным оценкам p_i. Таким образом, общая вероятность будет считаться по формуле

$$p\left(US.User's\_access\left(\overline{1..3}\right)\right) = 1-\left(1-p_1\right)\left(1-p_2\right)\left(1-p_3\right). \quad (1)$$

Таким же образом рассчитываются вероятности реакции пользователя на действия US.User's_access (предложение зарегистрироваться на каком-то привлекательном сайте) и US.User's_access (виртуальное знакомство с пользователем в сети).

Кроме того, очевидным образом из всех действий злоумышленника выделяются два итоговых состояния, в которые может прийти злоумышленник. Он может получить идентификационные данные пользователя, или же он получит доступ к компьютеру пользователя. Формула для общей вероятности получения идентификационных данных приведена ниже.

$$p\left(get\_US.id\right) = 1-\left(1-p_1\right)...\left(1-p_n\right),$$

где n — это количество $US.User's\_access\left(\overline{1..k}\right)$, которое ведет к получению идентификационных данных пользователя.

Рассмотрим формальное представление действий злоумышленника, направленных против информационной системы с учетом ответных действий пользователя.

У нас есть $A_n \in A$, где это множество атомарных атакующих действий злоумышленника, $B_n \in B$, где — множество атомарных ответных реакций пользователя.

Текущая ответная реакция пользователя $C^{B_k}_{\mathrm{US}(j)} = \mathrm{var}\left(A_i, \mathrm{US}(j), B_k\right)$

Функция $\mathrm{var}: A_n \times \mathrm{US} \times B_n \longrightarrow C^{B_k}_{\mathrm{US}(j)}$ ставит в соответствие конкретное атакующее действие злоумышленника, конкретного пользователя и конкретные ответные действия пользователя.

Формально, в общем виде, атака злоумышленника на пользователей представляет собой машину состояний

$$\Theta = \left\{ S^{\Theta}, A_{\overline{1..n}}, B_{\overline{1..n}}, p^{l}_{i,j}\left(B_i \middle| A_j\right), \mathrm{doc}^{\Theta}, p_k\left(\mathrm{doc}^{\Theta}_k \middle| p^{l}_{i,j}\left(B_i \middle| A_j\right)\right), \mathrm{US}_{\overline{1..n}}, \mathrm{tr} \right\},$$

где S^{Θ} — множество состояний, отображающих текущее положение в системе: какие действия совершены злоумышленником, против каких пользователей, какие действия пользователи осуществили в ответ, и какие документы злоумышленник добыл. $A_{\overline{1..n}}$ — множество совершенных злоумышленником действий. $B_{\overline{1..n}}$ — множество ответных реакций пользователя. $p^{l}_{i,j}\left(B_i \middle| A_j\right)$ — вероятность совершения пользователем US_l ответного действия B_i на атакующее действие злоумышленника A_j. Данная вероятность находится с помощью экспертно полученной шкалы на основе профиля уязвимостей пользователя. doc^{Θ} — набор доступных злоумышленнику критических документов в текущем состоянии атаки. $p_k\left(\mathrm{doc}^{\Theta}_k \middle| p^{l}_{i,j}\left(B_i \middle| A_j\right)\right)$ — вероятность того, что документ doc^{Θ}_l станет доступен злоумышленнику в случае атаки злоумышленника на пользователя US_l. $\mathrm{US}_{\overline{1..n}}$ — множество уже атакованных злоумышленником пользователей. tr — функция перехода из состояния в состояние $\mathrm{tr}: S^{\Theta} \longrightarrow S^{\Theta}$. При вызове данной функции происходит элементарное атакующее действие злоумышленника A_j на пользователя US_l, которое ведет к ответной реакции B_i и соответствующему пересчету всех вероятностей данной системы.

На следующем этапе планируется ввести расчет ущерба, нанесенного системе на основе вероятностей получения злоумышленником доступа к критичным документам $p_k\left(\mathrm{doc}^{\Theta}_k \middle| p^{l}_{i,j}\left(B_i \middle| A_j\right)\right)$. Такая вероятностная оценка позволяет не только предположить какой ущерб будет нанесен компании в том или ином случае, но и понять, какие именно пользователи подвержены тем или иным видам социо-инженерных атак. Такие показатели можно найти с помощью предположения, что чем выше вероятность, тем выше проявление уязвимости пользователя и, наконец, тем больше пользователь подвержен A_j виду социо-инженерных атак.

5. Прототип программного комплекса для анализа защищенности пользователей информационных систем. На основе вышеперечисленных информационных моделей разработан программный комплекс, позволяющий создавать информационные системы, а также рассчитывать вероятность того или иного действия пользователя в ответ на атакующее воздействие злоумышленника, а также рассчитать общую вероятность получения злоумышленником идентификационных данных пользователя.

Фрагмент профиля уязвимостей пользователя строится на основе психологических особенностей пользователя, которые могут быть выявлены на основе классического анкетирования, предназначенного для создания психологического портрета человека. Для того чтобы перевести психологические особенности пользователей в фрагмент профиля уязвимостей, была разработана специальная программа, проводящая перерасчет одних характеристик в другие. Данный перерасчет производится с помощью выявленных на этапе обработки результатов анкеты регрессионных уравнений.

Программа позволяет выбирать того или иного пользователя из базы данных, вероятность ответных действий которого необходимо рассчитать. При этом происходит имитация элементарных атакующих действий злоумышленника на выбранного пользователя, рассчитываются вероятности ответных действий пользователя, и выясняется вероятность получения злоумышленником идентификационных данных пользователя.

При запуске программы появляется первичный интерфейс (представлен на рисунке 1). Перед тем, как начать имитацию атак на пользователей информационной системы, необходимо создать информационную систему или загрузить базу данных с характеристиками уже созданной автоматизированной информационной системы.

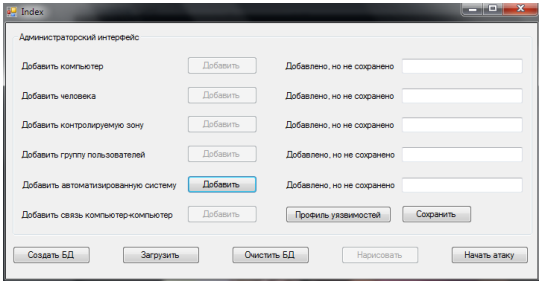

Рис. 1. Первичный интерфейс.

После того, как персональные данные пользователя и его уязвимости загружены в программу, можно приступать к построению атаки на него. Для этого нужно нажать кнопку «Начать атаку». В результате чего откроется новое диалоговое окно, изображенное на рис.2

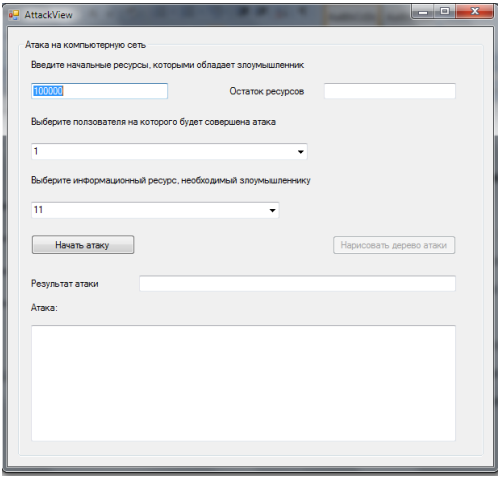

Рис. 2. Диалоговое окно «Атака».

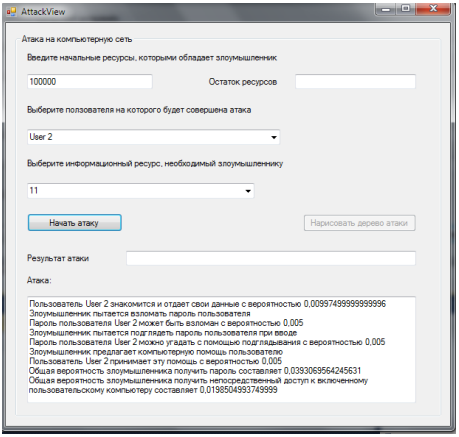

Рис. 3. Атака на пользователя User 2.

После этого необходимо выбрать пользователя, на которого будет совершена атака и нажать кнопку «Начать атаку», и программа выдаст результат, например, как на рис.3.

В данном примере злоумышленник получит идентификационные данные пользователя User2 с общей вероятностью 4%. Такие данные были получены при самых низких значениях уязвимостей.

6. Заключение. В данной статье рассмотрен подход к анализу защищенности пользователей информационных систем, построенный на основе известного формализма «деревья атак». Предложены информационные модели, задающие автоматизированную информационную систему, а также пользователей данных систем. Кроме того, существенным нововведением стало то, что информационные модели пользователей содержат фрагмент профиля уязвимостей пользователя, который построен на психологических особенностях пользователей, которые могут быть получены с помощью стандартного анкетирования, проводимого при приеме большинства сотрудников на работу. Таким образом, нет необходимости в проведении дополнительного анкетирования при проведении подготовительной работы, необходимой для анализа защищенности пользователей информационных систем. Созданный программный комплекс позволяет проводить вероятностный анализ защищенности пользователей информационных систем. В дальнейшем планируется доработать предложенный подход и привести данные информационные модели к реляционно-алгебраическому подходу для повышения быстродействия всего программного комплекса в целом.

Литература

1. *Азаров А.А., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л.* Развитие методов и моделей анализа защищенности информационных систем от социоинженерных атак на основе применения реляционно-алгебраических представлений и алгоритмов // VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2011)» (Санкт-Петербург, 26–28 октября 2011 г.) Материалы конференции. СПб.: СПОИСУ, 2011. С. 160-161.

2. *Азаров А. А., Тулупьева Т.В., Тулупьев А.Л., Пащенко А.Е.* Создание программного комплекса для анализа защищенности информационных систем с учетом человеческого фактора. // Современные информационные технологии и ИТ-образование. Сборник научных трудов VI Международной научно-практической конференции. М: МГУ. 2011. С. 470-477.

3. *Ванюшичева О.Ю.* Прототип комплекса программ для построения профиля психологически обусловленных уязвимостей пользователя. Дипломная 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 интен-

сивности 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. *Степашкин М.В.* Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак: Дис. канд. техн. наук: СПб.: СПИИРАН, 2002. 196 с.

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 инфосферысистем критических приложений. Вооружение. Политика. Конверсия. 2003. № 2. С. 52.

22. *Dorothy E. Denning* A Lattice Model of Secure Information Flow. // Communications of the ACM, 2008, Vol. 19, No. 5, pp. 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, pp. 135-154 (2003)

24. *Jahnke, M., Thul, C., Martini, P*. Graph based metrics for intrusion response measures in computer networks. LCN 2007: Proceedings of the 32nd IEEE Conference on Local Computer Networks, Washington, DC, USA, pp. 1035-1042. IEEE Computer Society, Los Alamitos (2007)

25. *Toth, T., Krugel, C*. Evaluating the impact of automated intrusion response mechanisms. ACSAC 2002: Proceedings of the 18th Annual Computer Security Applications Conference, Washington, DC, USA, p. 301. IEEE Computer Society, Los Alamitos (2002)

Азаров Артур Александрович — м.н.с., лаборатория теоретических и междисциплинарных проблем информатики, СПИИРАН. Область научных интересов: защита информации, анализ защищенности информационных систем. Число научных публикаций — 20. 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 — 20. 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.

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.

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 sociocultural 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.

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.

Рекомендовано лабораторией теоретических и междисциплинарных проблем информатики, заведующий лабораторией Тулупьев А.Л., д.ф-м.н., доц.
Статья поступила в редакцию 05.05.2012.

РЕФЕРАТ

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.**

Комплексные корпоративные информационные системы в настоящее время получают все большее распространение в современном мире. Разработка, поддержка и защита подобных систем занимает значительное количество времени и ресурсов, кроме того только высококвалифицированные специалисты могут заниматься подобными системами. Информация, хранимая в таких информационных системах, имеет огромную ценность для компаний-владельцев систем, поэтому значительные усилия затрачиваются на построение системы защиты таких систем от различных угроз безопасности. Новейшие системы безопасности могут защитить информационные системы от большинства кибер-атак (т.е. программно-технических), а также серьезно осложнить жизнь злоумышленникам, пытающимся добраться до конфиденциальной информации, но в то же время большинство таких систем не защищено от внутренних угроз, исходящих от их пользователей. Таким образом, злоумышленники, обладающие навыками социо-инженеров, с легкостью могут повлиять на пользователей информационных систем с целью получения именно той информации, которая им нужна.

Необходимо научиться защищать информацию от такого типа атак (т.е. социо-инженерных атак или социотехнических атак). Кроме того необходимо научиться оценивать уровень защищенности персонала информационных систем от социо-инженерных атак. То есть, поскольку подобные атаки используют пользователей информационных систем в качестве основного пути развития атаки, необходимо научиться прогнозировать уязвимости пользователей информационных систем, а также строить агрегированные, сводные показатели защищенности или уязвимости персонала «в целом».

Целью данной статьи является комбинация нечеткого и вероятностного подхода к оценке защищенности пользователя по отношению к атакующим действиям злоумышленника, причем рассматриваются действия достаточно элементарного характера («одноходовки»), нацеленные на «элементарные» уязвимости пользователя, воздействие на которые приводит непосредственно к какому-то действию пользователя.

SUMMARY

Azarov A.A., Tulupyeva T.V., Tulupyev A.L. **Software prototype for information systems' personnel's protection analysis based on the fragment of user's vulnerabilities profile.**

Complex corporate information systems gain ground now in the modern world. Development, support and protection of similar systems demand a significant amount of time and resources, besides only highly skilled experts can be engaged in the supporting of these systems. Information stored in such information systems has enormous value for the companies owners of systems therefore considerable efforts are spent for creation of system of protection of such systems from various threats of safety. The newest systems of safety can protect information systems from the majority a cyber attacks (i.e. program and technical), and also seriously complicate the lives of malefactors who try to obtain confidential information, but at the same time the majority of such systems isn't protected from the internal threats proceeding from the users of such systems. Thus, the malefactors possessing skills of social engineers with ease can affect users of information systems for the purpose of obtaining that information which is necessary to them.

It is necessary to learn to protect information from attacks of this kind (i.e. socio-engineering attacks or sociotechnical attacks). Besides it is necessary to learn to estimate the level of security of the personnel of information systems from socio-engineering attacks. That is, as those attacks are aimed at the users of information systems as the main way of development of attack, it is necessary to learn to predict vulnerabilities of users of information systems, and also to build the aggregated, summary indicators of security or vulnerability of the personnel "as a whole".

The purpose of this paper is to combine indistinct and likelihood approaches to an assessment of security of the user in relation to attacking actions of the malefactor, and the actions of rather elementary character ("one movement") aimed at "elementary" vulnerabilities of the user which lead directly to some action of the user are considered.