УДК 614.8 + 002.6:004.89

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

ВЕРОЯТНОСТО-РЕЛЯЦИОННЫЙ ПОДХОД К ПРЕДСТАВЛЕНИЮ МОДЕЛИ КОМПЛЕКСА «ИНФОРМАЦИОННАЯ СИСТЕМА – ПЕРСОНАЛ – КРИТИЧНЫЕ ДОКУМЕНТЫ»

Азаров А.А., Тулупьева Т.В., Фильченков А.А., Тулупьев А.Л. **Вероятностно-реляционный подход к представлению модели комплекса «Информационная система – персонал – критичные документы».**

Аннотация. Одной из основных проблем исследований в области социо-инженерных атак является развитие приемлемых по вычислительной сложности алгоритмов анализа (оценки) защищенности персонала информационных систем. По предварительным оценкам именно применение вероятностно-реляционного алгоритма поможет существенно уменьшить вычислительную сложность программного комплекса. Использование указанного подхода позволит также увеличить гибкость в задании оценок критичности документов, доступных в системе, оценок шансов успешной реализации атак, описании системы связей и доступа среди собственно компонент комплекса «информационная система – персонал – критичные документы» и среди указанных компонент, и злоумышленника. Реляционные модели, возможно, позволят при вычислениях оценок степени защищенности использовать вычислительные методы, которые эффективно реализованы в современных СУБД для быстрого выполнения SQL-запросов.

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

Azarov A.A., Tulupyeva T.V., Filchenkov A.A, Tulupyev A.L. **Probabilistic relational approach to representing "informational system – personnel – critical documents" complex model.**

Abstract. One of the main problems of researches in the field of socio-engineering attacks is the development of analysis algorithms (assessment) of information system's users' protection estimated on the basis of computing complexity. According to preliminary estimates the application of probabilistic relational algorithm will essentially reduce computing complexity of a program complex. Use of the specified approach will also allow to increase flexibility in a task of estimation of criticality of the documents available in system and chances of successful realization of attacks, in description of communications' system and accesses among actual components of a complex «information system – personnel – critical documents», and among specified components and the malefactor. Relational models will probably allow to use effective computational methods, implemented in modern DBSM for fast SQL-links implementation.

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

1. Введение. Одной из основных проблем исследований в области социо-инженерных атак является, с одной стороны, разработка подходящих для последующего анализа степени защищенности моделей информационных систем, персонала, набора критичных документов, злоумышленника, а также разнообразных связей между указанными сущностями, а с другой стороны — развитие приемлемых по вычисли-

тельной сложности алгоритмов анализа (оценки) защищенности персонала информационных систем. Ожидается [5], что дополнение (либо даже замена) системы переборных алгоритмов реляционно-алгебраическим подходом (и впоследствии на его основе — реляционно-вероятностным подходом) к представлению исходных данных и организации вычислений позволит уменьшить время обработки сведений об информационной системе и ее персонале, а также время, затрачиваемое на построение набора возможных атак. Использование указанного подхода позволит также увеличить гибкость в задании оценок критичности документов, доступных в системе, оценок шансов успешной реализации атак, описании системы связей и доступа среди собственно компонент комплекса «информационная система – персонал – критичные документы» и среди указанных компонент, и злоумышленника. Наконец, реляционно-алгебраический подход позволяет использовать стандартный инструментарий реляционных баз данных для представления данных в автоматизированных системах анализа защищенности, что в свою очередь может открыть путь к вычислению оценки защищенности на основе SQL-запросов, исполнение которых автоматически распараллеливается и оптимизируется встроенной функциональностью современных СУБД.

Цель статьи — представить основы подхода к алгоритмизации анализа защищенности персонала информационной системы от социоинженерных атак, базирующиеся на реляционно-алгебраическом и — более общем — вероятностно-реляционном подходе. Последний, в свою очередь, допускает адаптацию к использованию не только вероятностных, но и нечетких оценок (а также, возможно, оценок, опирающихся на иные подходы к формализации степеней доверия) для представления неопределенности знаний об анализируемом комплексе и атакующем его злоумышленнике.

В качестве «отправной точки» предлагается использовать модель комплекса «информационная система – персонал – критичные документы», в которой информационная система представлена в виде графа, узлы которого отвечают программно-техническим компонентам системы, а ребра — связям между такими компонентами[4, 9]. Причем как узлам, так и дугам сопоставлены достаточно богатые информационные модели соответствующих сущностей. Сложноустроенные угрозообразующие воздействия на информационную систему в рамках рассматриваемой базовой модели представляются в виде деревьев атак. В этом случае, анализ степени защищенности информационной системы сводится к анализу набора возможных деревьев атак [15]. (В краткой

формулировке процесс выглядит достаточно просто; что, однако, не упрощает ни само исследование вовлеченных объектов и процессов, ни сбор необходимой для оценки информации, ни разработку комплексов программ, формирующих оценку защищенности.)

Для обобщения указанного подхода для комплекса «информационная система—персонал» потребуется разработать ряд моделей (математических, информационных, визуальных и проч.) позволяющих учесть новую подсистему —«персонал» — и ее компоненты, связи внутри этой новой подсистемы, связи между подсистемами «персонал» и «информационная система», связи этих подсистем с внешней средой (прежде всего, имеются в виду лица, действия которых составляют или могут составлять угрозу для безопасности информации, хранящейся в информационной системе).

Кроме того, данный подход может быть применен к полученным в ходе социологического исследования психологическим уязвимостям пользователя.

2. Реляционный подход Н.В. Хованова. Н.В. Хованов, обобщая и адаптируя в [22] результаты и положения ряда общетеоретических, частных и учебных публикаций, предложил моделировать комплекс «товар – посредник – потребитель» на основе реляционного подхода. Под товаром понимается некоторое экономическое благо, циркулирующее на рынке.

В простейшем случае, согласно [22], товар характеризуется вектором $v = (c, u, p)$, где c — градация производственной ценности товара, u — градация потребительской ценности и, наконец, p — градация меновой ценности. Каждый компонент вектора v измеряется в определенной шкале (C, U, P соответственно), которая полагается конечной и дискретной.

В детерминированном случае возможность перехода товара от производителя к посреднику характеризуется отношением $R_1(c, p)$ — подмножеством декартова произведения $C \times P$, возможность перехода товара от посредника к потребителю — отношением $R_2(p, u)$ (подмножество декартова произведения $P \times U$), и, наконец, существенным ограничением на обмен является отношение $R_3(c, u)$ — подмножество декартова произведения $C \times U$. Распространение модели на случай нескольких посредников может быть реализовано введением нескольких отношений $R_{2i}(p_i, u_i)$, где i индексирует множество посредников,

для первого посредника $P_i = P$, для последнего посредника $U_i = U$, а в отношениях между посредниками $P_{i+1} = U_i$; соответственно задаются и декартовы произведения доменов.

На основе отношений R_1, R_2, R_3 строится отношение $R_1(c,u,p)$, которое и характеризует возможность того, что товар при заданных сочетаниях градаций перейдет от производителя покупателю. В стохастическом случае при некоторых предположениях вычисляется вероятность такого перехода.

3.Реляционно-алгебраическая модель комплекса «информационная система – персонал». Указанный подход можно адаптировать к представлению отношений в комплексе «информационная система – персонал», приняв во внимание необходимые доработки и количественные измерения угрозообразующего поведения человека, сделанные в [1-2, 4-9, 11-20 12-21, 23-26]. С точки зрения анализа защищенности от социо-инженерных атак, в указанном комплексе можно выделить следующие компоненты: I — критичная информация, более точно — система документов, каждый из которых, с одной стороны, характеризуется показателем или показателями критичности, а с другой стороны, атрибутами, характеризующими его доступность с такого-то хоста с правами такого-то пользователя; H — хосты, которые характеризуются своими связями с другими хостами, рядом атрибутов, описывающих текущую конфигурацию программно-технического обеспечения (по этим атрибутам определяется успешность реализации атакующих действий программно-технического характера), а также рядом атрибутов, описывающих права пользователей на данном хосте; U — пользователи, которые характеризуются своими связями с группами пользователей, в отношении которых установлены определенные политики безопасности, допуски в определенные зоны, а также профили уязвимости (которые формируются, в том числе, на основе сведений о психологической защите), причем профиль уязвимости определяет вероятность успеха социо-инженерных атакующих действий, и связями с другими пользователями; A — атакующие действия, предпринимаемые злоумышленником или группой злоумышленников, которые могут быть направлены как на пользователей, так и на хосты, каждому из которых, в свою очередь, задан вес, который отражает требуемые для осуществления данного атакующего действия ресурсы. Поскольку атаки на хосты рассматривались в работах, систематический обзор которых можно найти, например, в [14, 18-20, 26], то в

данном докладе мы формализуем лишь атаки на пользователя. Такая модель легко генерализуется и для общего случая.

Отношения между элементами указанных компонент допускают формализацию тем же путем, как это было выполнено в [22], но семантика таких отношений будет иной, отражающей особенности предметной области.

4. Вероятностно-реляционная модель атакующих действий. Прежде всего, рассмотрим модель атакующих действий для того, чтобы сформулировать соглашения и описать возможности, которые мы будем подразумевать при описании остальных элементов системы.

Каждая атака требует определенное число ресурсов. Ресурсами могут выступать как денежные средства, так и богатый спектр других средств (возможности психологического, социального, технико-инженерного воздействий).

В упрощенной модели мы можем ввести дискретную шкалу R, которая будет измерять количество требуемых ресурсов. В современных условиях подобное допущение вполне отвечает существующей системе, поскольку финансовые ресурсы могут быть в известной степени конвертированы в любой другой ресурс.

Более сложная модель предполагает использование многомерной шкалы $\boldsymbol{R} = R_1 \times \ldots \times R_n$, где R_i — дискретная шкала измерения конкретного ресурса. Примерами такой многомерной шкалы могут выступать шкалы, измеряющие финансовые средства и затрачиваемое время или финансовые средства, усилия эксперта по психологическому воздействию (психолога), усилия эксперта по техническому воздействию (хакера). Однако следует сразу указать на ряд недостатков усложненной модели. Во-первых, в силу того что ресурсы скорее всего частично конвертируемы, следует выделить классы эквивалентности различных многомерных измерений, что значительно усложняет модель. Во-вторых, из теории управления известно, что сложность управления подобной системой растет очень быстро при увеличении числа моделируемых ресурсов, что заставляет делать выбор между точностью представления и операбельностью модели. Далее мы будем говорить про шкалу R, которую можно рассматривать как одномерной, так и многомерный с учетом сделанных выше предположений.

Рассмотрим отношение $A_U(a,u)$, которое задают возможности проведения атаки a на пользователя u. $(a,u) \in A_U$ говорит о том, что атака a будет воздействовать на пользователя u. $R_{AU} : A_U \to R$ задает

число ресурсов, которые необходимо потратить на соответствующую атаку.

Более общим случаем будет являться ввод на декартовом произведении $A \times U$ функции p_{AU}, которая определяет вероятность успешности атаки. Для тех пар, которые не входят в A_U, эта вероятность окажется тождественно равной нулю (либо же меньше заранее заданной величины).

Наиболее общим случаем будет введение функции p_{AUR}, заданной на декартовом произведении $A \times U \times R$, которая определяется вероятность успешности данной атаки на данного пользователя при использовании данного количества ресурсов.

5. Вероятностно-реляционная модель комплекса «информационная система – персонал». $H_I(h,i)$ — подмножество декартового произведения $H \times I$, которое отображает возможность прямого доступа с хоста h к критичному документу i. В графовой модели подобное отношение формализуется через наличие ребра от вершины h до вершины i. Так, например, $(h,i) \in H_I$, когда i хранится на h.

$U_H(u,h)$ — подмножество декартового произведения $U \times H$, которое отображает непосредственную возможность доступа пользователя u к хосту h. В упрощенной (детерминированной) модели мы предполагаем, что пользователь либо имеет, либо не имеет доступ к соответствующему хосту. В графовой модели подобное отношение формализуется через наличие ребра от вершины u до вершины h. Так, например, $(u,h) \in U_H$, когда u работает за компьютером h.

Рассмотрим декартово произведение $H \times H$. Можно ввести либо отношение $A_H(h_1,h_2)$, которое характеризует непосредственный доступ от одного хоста до другого (связь в сеть, и т.д.), либо вероятность $p_H(h_1,h_2)$, задающую вероятность такого доступа.

Сходные A_U или p_U можно задать и для декартового произведения $U \times U$ (например, дружеские контакты, служебные отношения, и т.д.)

Вариантом обобщения модели будет также введение ресурсных функций (т.е., например, финансовые средства могут быть переданы пользователю, чтобы он подкупил другого пользователя, с которым он состоит в дружеских отношениях), которые будут определять стоимость атак, однако в рамках данной работы мы будем считать, что по-

добные стратегии уже закладываются в понятие «атака» и описываются множеством A, и ее ресурсная оценка уже включает все дальнейшие перераспределения ресурсов в рамках взаимодействия между другими узлами.

Благодаря введенным выше понятиям мы можем формализовать понятие *достижимости*.

Так, в детерминированном случае критическая информация i *достижима* из хоста h, если существует такой упорядоченный набор хостов $h_1,\ldots,h_n$, что (h,h_1), (h_1,h_2), …, $(h_{n-1},h_n) \in A_H$ и $(h_n,i) \in H_I$. Будем обозначать это отношением $\mathrm{ATT}_H(h,i)$. Аналогичное отношение для *достижимости* хоста h пользователем u будем обозначать как $\mathrm{ATT}_U(u,h)$ (в этом случае требуется набор пользователей с соответствующими отношениями). В графовой модели подобное отношение характеризуется достижимостью вершины i из вершины h (h и u соответственно для пользователя).

В случае, если была задана функция p_H, вводится функция $P_H(h,i)$, которая определяется следующим образом:

$$P_H(h,i) = \sum_{\{h_i\}_n} \left(\prod_{\substack{j: h_j, h_{j+1} \in \{h_i\} \\ (h_n,i) \in H_I}} p_H(h_j, h_{j+1}) \right),$$

т.е. произведение вероятностей всех ребер на всех путях, которые ведут от h до i.

Аналогичным образом можно ввести функцию $P_U(u,h)$.

В детерминированном случае *достижимость* $\mathrm{ATT}_I(u,i)$ информации i пользователем u определяется существованием такой пары $(u_a,h_a) \in U_H$, что $(u,u_a) \in \mathrm{ATT}_U$ и $(h_a,i) \in \mathrm{ATT}_H$.

В случае, если мы задали функции вероятности, то введем вероятность достижения информации i пользователем u следующим образом:

$$P_I(u,i) = \sum_{\substack{u_a \in U, \\ (u_a,h_a) \in U_H}} P_U(u,u_a) \cdot P_H(h_a,i).$$

6. Пример социо-инженерной атаки злоумышленника на пользователей информационной системы. Рассмотрим модель взаимодействия информационной системы, пользователей и злоумышленника, которая была описана в п. 3-5 данной статьи. То есть, имеется информационная система, состоящая из устройств-хостов (компьютеры, роутеры, хабы и пр.) H. На данных устройствах, а также в сети, образованной данными устройствами, хранится определенная информация, состоящая из набора критичных документов, каждый из которых имеет свою ценность — I. Кроме того, в данной информационной системе работает персонал, имеющий различный уровень доступа к хостам, различные взаимоотношения внутри коллектива, и, наконец, различный уровень проявления уязвимостей у каждого пользователя. Данное множество пользователей обозначено через U.

При совершении злоумышленником социо-инженерной атаки A на пользователей информационных систем происходит расчет вероятности успешности завершения данной социо-инженерной атаки, которая обозначается через p_{AU}, атака считается успешно завершенной, если злоумышленнику удалось склонить на свою сторону пользователя (например подкупить). При успешно проведенной атаке пользователь пытается достать тот критический документ, который нужен злоумышленнику. Для этого пользователь смотрит на доступных ему компьютерах, есть ли на нем данный критичный документ. Данные зависимости обусловлены отношениями $U_H(u,h)$ (находим те устройства, к которым у пользователя есть доступ) и $H_I(h,i)$ (на конкретном устройстве есть искомый критичный документ).

Если необходимый злоумышленнику документ не найден пользователем, то пользователь пытается воспользоваться своими связями с другими пользователями, чтобы также включить их во множество скомпрометированных злоумышленником пользователей. Нахождение данных пользователей происходит с помощью p_U. При нахождении нового пользователя на него также совершается социо-инженерная атака A. Происходит новая итерация атакующего воздействия злоумышленника, которая происходит по тому же принципу, который был изложен выше.

Таким образом, итоговое состояние социо-инженерной атаки может быть получено или при получении необходимого злоумышленнику критического документа, или при переборе всех возможных пользователей, или при недостающих ресурсах злоумышленника.

7. Построение профиля уязвимостей. Степень проявления уязвимостей пользователя. Еще на начальных этапах исследования моделей комплекса «информационная система – персонал – критичные документы» нами была сформулирована задача перехода от профиля психологических особенностей пользователя к профилю его уязвимостей. Было выдвинуто предположение, что степени уязвимостей пользователя являются латентными переменными, соответственно они могут быть выявлены при использовании одного из вариантов метода главных компонент; причём затем такие выявленные латентные переменные могут быть предсказаны с помощью регрессионных уравнений, где предикторами выступали бы степени выраженности психологических особенностей пользователя. К построению таких уравнений удалось приблизиться с помощью результатов пилотного исследования [3].

Благодаря данному исследованию было выявлено 5 уязвимостей пользователя (ожидается, что таких уязвимостей, конечно, впоследствии, в более широкомасштабных исследованиях будет обнаружено больше), а также была получена привязка степени проявления данных уязвимостей к степени выраженности психологических особенностей пользователя. Данные уязвимости составили фрагмент профиля уязвимостей пользователя, который необходим для анализа защищенности пользователей информационных систем от социо-инженерных атак. Также экспертным путем был выявлен перечень элементарных атакующих действий злоумышленника, которые могут эксплуатировать данные уязвимости пользователя.

Опираясь на профиль уязвимостей, можно оценить вероятность успешной реализации атакующего воздействия злоумышленника на пользователя. Это открывает возможность как для адаптации известного подхода анализа деревьев атак для агрегированной оценки степени защищенности персонала информационных систем от социо-инженерных атак, так и для использования предлагаемого в настоящей работе реляционно-вероятностного подхода в тех же целях [3].

8.Заключение. Благодаря введенным определениям и объектам, мы можем (в зависимости от построенной модели) исследовать возможности атак, вероятности их успешной реализации, затраты ресурсов злоумышленника, а также дать агрегированную оценку степени защищенности интересующего нас комплекса от социо-инженерных атак.

Предложенный в работе вероятностно-реляционный подход позволяет не только весьма удачно формализовать «на бумаге» рассмат-

риваемую модель с помощью классического инструментария реляционных алгебр, теории вероятностей, теории нечеткости (и, на самом деле, теорий иных степеней доверия), но и открывает перспективы непосредственного использования указанной формализации при сведении модели очень сложных сущностей (комплекса «информационная система – персонал – критичные документы», взаимодействий этого комплекса и злоумышленника, набора возможных атак и др.) к системе таблиц в реляционной базе данных, а вопросы организации и — что особенно важно — ускорения вычислений оценки степени защищенности — к формированию SQL-запросов, которые оптимизируются современными СУБД самостоятельно.

Наконец, необходимо отметить, что хотя представленная вероятностно-реляционная модель сама по себе является гибридной, она допускает свое дальнейшее развитие в сторону применения методов теории нечеткости и теорий, обслуживающих другие степени доверия.

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 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. *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. *Хованов Н.В.* Общая модель измерения ценности экономических благ // Применение математики в экономике. Вып. 18 / Под. ред. Воронцовского А.В. СПб.: «ИПК «КОСТА», 2009. С.108-134

22. *Юсупов Р., Пальчун Б.П.* Безопасность компьютерной инфосферы систем критических приложений. Вооружение. Политика. Конверсия. 2003. № 2. С. 52.

23. *Dorothy E. Denning* A Lattice Model of Secure Information Flow. // Communications of the ACM, 2008, Vol. 19, No. 5, pp. 236–243

24. *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)

25. *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)

26. *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 systems' 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.

Фильченков Андрей Александрович — младший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики, СПИИРАН. Область научных интересов: автоматическое обучение вероятностных графических моделей. Число научных публикаций — 50.aaafil@mail.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.

Filchenkov Andrey Alexandrovich — junior researcher, Theoretical and Interdisciplinary Computer Science Laboratory, SPIIRAS. Research interests: machine learning of probabilistic graphical models. The number of publications — 50. aaafil@mail.ru, www.tulupyev.spb.ru; SPIIRAS, 39, 14-thLine V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

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

Tulupyev Alexander Lvovich — Dr. Sc. in Physics and Mathematics, associate professor; head of Laboratory of Theoretical and Interdisciplinary Computer Science, SPIIRAS, associate professor, Computer Science Department, Faculty of Mathematics and Mechanics, SPbSU. Research interests: uncertain knowledge and data representation and processing, application of mathematics and computer science in 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 20.03.2012.

РЕФЕРАТ

Азаров А.А., Тулупьева Т.В., Фильченков А.А., Тулупьев А.Л. **Вероятностно-реляционный подход к представлению модели комплекса "Информационная система – персонал – критичные документы".**

Одной из основных проблем исследований в области социо-инженерных атак является развитие приемлемых по вычислительной сложности алгоритмов анализа (оценки) защищенности персонала информационных систем. Ожидается, что дополнение (либо даже замена) системы переборных алгоритмов реляционно-алгебраическим подходом к представлению исходных данных и организации вычислений позволит уменьшить время обработки сведений об информационной системе и ее персонале, а также время, затрачиваемое на построение набора возможных атак. Использование указанного подхода позволит также увеличить гибкость в задании оценок критичности документов, доступных в системе, оценок шансов успешной реализации атак, описанию системы связей и доступа среди собственно компонент комплекса «информационная система – персонал – критичные документы», и среди указанных компонент и злоумышленника. Наконец, реляционно-алгебраический подход позволяет использовать стандартный инструментарий реляционных баз данных для представления данных в автоматизированных системах анализа защищенности, что, в свою очередь, может открыть путь к вычислению оценки защищенности на основе SQL-запросов, исполнение которых автоматически распараллеливается и оптимизируется встроенной функциональностью современных СУБД.

Цель статьи — представить основы подхода к алгоритмизации анализа защищенности персонала информационной системы от социоинженерных атак, базирующиеся на реляционно-алгебраическом и — более общем — вероятностно-реляционном подходе. Последний, в свою очередь, допускает адаптацию к использованию не только вероятностных, но и нечетких оценок для представления неопределенности знаний об анализируемом комплексе и атакующем его злоумышленнике.

В качестве «отправной точки» предлагается использовать модель комплекса «информационная система – персонал – критичные документы», в которой информационная система представлена в виде графа, узлы которого отвечают программно-техническим компонентам системы, а ребра — связям между таким компонентами. Причем как узлам, так и дугам сопоставлены достаточно богатые информационные модели соответствующих сущностей. Сложноустроенные угрозообразующие воздействия на информационную систему в рамках рассматриваемой базовой модели представляются в виде деревьев атак. В этом случае, анализ степени защищенности информационной системы сводится к анализу набора возможных деревьев атак.

SUMMARY

Azarov A.A., Tulupyeva T.V., Filchenkov A.A, Tulupyev A.L. **Probabilistic relational aprroach to representing "informational system – personnel – critical documents" complex model.**

One of the main problems of researches in the field of socio-engineering attacks is the development of analysis algorithms (assessment) of information system's users' protection estimated on the basis of computing complexity. It is expected that addition (or even replacement) of search algorithms systems by relational and algebraic approach to representation of basic data and the organization of calculations will allow to reduce the time of data processing in information system and it's personnel, and also the time spent for creation of a set of possible attacks. Use of the specified approach will also allow to increase flexibility in a task of estimation of criticality of the documents available in system and chances of successful realization of attacks, in description of communications' system and accesses among actual components of a complex «information system – personnel – critical documents», and among specified components and the malefactor.

At last, the relational and algebraic approach allows to use standard tools of relational databases for data presentation in the automated systems of the analysis of security that in turn can open a way to calculation of security assessment on the basis of the SQL inquiries which is held automatically simultaneously and is optimized by the built-in functionality of modern DBMS.

The aim of the report is to present approach bases to algorithmization of the analysis of security of the personnel of information system from the socio-engineering attacks, based on relational and algebraic and — more general — on probabilistic and relational approach. The last, in turn, allows adaptation to use not only probabilistic, but also an indistinct estimates for idea of uncertainty of knowledge of an analyzed complex and the malefactor attacking it.

As "starting point" it is offered to use complex model «information system – personnel – critical documents» in which information system is presented in the form of the count which knots answer program and technical components of the system, and edges — to communications between such components. And rich information models of the corresponding base are compared with both knots and arches. Injuring impacts on information system within considered base model are represented in the form of trees of attacks. In this case, the analysis of degree of security of information system comes to the analysis of a set of possible trees of attacks.