УДК 614.8 + 002.6:004.89

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

SQL-ПРЕДСТАВЛЕНИЕ РЕЛЯЦИОННО-ВЕРОЯТНОСТНЫХ МОДЕЛЕЙ СОЦИО-ИНЖЕНЕРНЫХ АТАК В ЗАДАЧАХ РАСЧЕТА АГРЕГИРОВАННЫХ ОЦЕНОК ЗАЩИЩЕННОСТИ ПЕРСОНАЛА ИНФОРМАЦИОННОЙ СИСТЕМЫ

Азаров А.А., Тулупьев А.Л., Тулупьева Т.В. **SQL-представление реляционно-вероятностных моделей социо-инженерных атак в задачах расчета агрегированных оценок защищенности персонала информационной системы.**

Аннотация. Анализ рисков информационной безопасности в настоящее время является особо актуальной темой, в силу того, что и страховые компании хотят иметь возможно более точные характеристики о вероятном размере ущерба и необходимой сумме страхования, и компании, желающие застраховать свои информационные риски, также хотят понимать, за что именно и насколько обоснованно платятся те или иные суммы при заключении договора страхования. Кроме того, ни одна из названных сторон не хочет терять собственные ресурсы. Таким образом, необходимо научиться получать адекватные, но в то же время комплексные, агрегированные оценки защищенности информационных систем. Целью настоящей статьи является рассмотрение варианта задания основных отношений в комплексе «персонал - информационная система – критичные документы» при социо-инженерной атаке злоумышленника, а затем иллюстрация работы принципов вероятностно-реляционного подхода на упрощенном (для доступности и краткости изложения) примере. Будем использовать смешанную терминологию, заимствованную из теории отношений и теории реляционных БД.

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

Azarov A.A., Tulupyev A.L., Tulupyeva T.V. **SQL representation of relational and probabilistic models of socio-engineering attacks in problems of calculation of the aggregated information system's personnel's security estimation.**

Abstract. Risk analysis of information security nowadays is an extremely important topic, due to the fact that insurance companies want to have probably more exact characteristics about the probable size of a damage and the necessary sum of insurance, and the company, wishing to insure the information risks, also wants to understand, for what it does pay at the conclusion of the contract of insurance and if these fees are reasonable. Besides, both mentioned above parties don't want to lose their resources. Thus, it is necessary to learn to receive adequate, but at the same time complex, aggregated estimates of security of information systems. The purpose of the present article is consideration of setting of general relations in a complex «the personnel information system – critical documents» at socio-engineering attack of the malefactor, and then illustration of work of principles of a likelihood and relational approach on simplified (for availability and brevity of a statement) example. We'll use the mixed terminology borrowed from the theory of the relations and the theory of relational DB.

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

1. Введение. Анализ рисков информационной безопасности в настоящее время является особо актуальной темой, в силу того, что и страховые компании хотят иметь возможно более точные характеристики о вероятном размере ущерба и необходимой сумме страхования,

и компании, желающие застраховать свои информационные риски, также хотят понимать, за что именно и насколько обоснованно платятся те или иные суммы при заключении договора страхования. Кроме того, ни одна из названных сторон не хочет терять собственные ресурсы. Таким образом, необходимо научиться получать адекватные, но в то же время комплексные, агрегированные оценки защищенности информационных систем. Для этого необходим всесторонний анализ защищенности как программно-технической составляющей системы, так и персонала таких систем (их социотехнической составляющей). Для оценки защищенности программно-технической составляющей информационных систем разработано множество методов, которые используются в существующих продуктах для автоматизации анализа защищенности указанных систем, например методологии NIST, OCTAVE, CRAMM[25–27]. Вместе с тем, методы анализа защищенности пользователей (и персонала в целом) мало освещены [21–24, 28] и остаются, видимо, мало исследованы специалистами из области информатики и информационной безопасности. Именно поэтому настоящая работа концентрируется на возможном подходе к автоматизации анализа защищенности пользователей информационных систем от социо-инженерных атак. Социо-инженерная атака рассматривается как реализация элементарных атакующих действий, направленных на уязвимости пользователя. Данный подход был рассмотрен в статьях [1, 2, 12–16]. Для разработки моделей, а затем — подходящих структур данных для реализации алгоритмов автоматизированного анализа защищенности от социо-инженерных атак было решено применить реляционно-алгебраический подход. Он позволяет, с одной стороны, перейти к отношениям для представления данных, то есть для представления модели контекста, в котором будут развиваться социо-инженерные атаки, и модели злоумышленника, и, с другой стороны, использовать эффективные алгоритмы обработки SQL-запросов, реализованные в современных СУБД, для вычисления искомых показателей — агрегированных оценок степени защищенности персонала либо степени «поражаемости» критичных документов при социо-инженерных атаках. Предлагаемые реляционные модели основаны на результатах, изложенных в [1].

Целью настоящей статьи является рассмотрение варианта задания основных отношений в комплексе «персонал - информационная система – критичные документы» при социо-инженерной атаке злоумышленника, а затем иллюстрация работы принципов вероятностно-реляционного подхода на упрощенном (для доступности и краткости

изложения) примере. Будем использовать смешанную терминологию, заимствованную из теории отношений и теории реляционных БД[4–13, 17-20].

2. Реляционные модели критических документов. К рассмотрению предлагаются две реляционные модели критических документов. Первая задает цену потери данных документов — document (id, price). Такая цена устанавливается владельцем информационной системы. Вторая модель формализует одно из возможных описаний политик организации доступа к таким критичным документам — document_access (id, id_document, id_user, id_comp, id_zone). В используемой нотации перед скобками идет идентификатор отношения. В качестве аргументов выступает серия атрибутов: id — это ключ базы данных для организации доступа к данному документу, id_document — это номер документа из document, id_user— это номер пользователя, доступ которого описывается в данном отношении, id_comp — компьютер, на котором хранится данный документ, id_zone — контролируемая зона, к которой относится устройство, на котором хранится документ. Отметим, что в рассматриваемом случае вторая реляционная модель представлена в простейшем виде. Она показывает доступ конкретного пользователя id_user, работающего на конкретном устройстве id_comp, находящегося в конкретной контролируемой зоне id_zone. Но, в тоже время, возможны иные подходы к описанию политик доступа. Например, если в качестве устройства задан мобильный компьютер (ноутбук, смартфон и так далее), то необходимо рассматривать доступ во множестве контролируемых зон, потому что устройство может быть перенесено и переподключено (переподсоединено к сети). Кроме того, пользователь может иметь доступ к нескольким стационарным устройствам, находящимся в одной контролируемой зоне и имеющим одинаковый порт подключения к сети подключения к сети. В таком случае целесообразно рассматривать группу компьютеров. Далее, к одному компьютеру могут иметь доступ сразу несколько пользователей, относящихся к одной группе пользователей и имеющих доступ к одному устройству. Тогда следует рассматривать группу пользователей. Наконец, возможны варианты, когда необходимо рассматривать по два или три вида таких групп сразу.

3.Реляционные модели исходных политик безопасности информационной системы. Для описания реляционных моделей исходных политик безопасности предлагается использовать 6 моделей. Среди них: модель групп пользователей, модель групп устройств, модель доступа групп пользователей в контролируемые зоны, модель доступа

групп пользователей к устройствам, модель принадлежности пользователей к группам пользователей, модель принадлежности технических устройств к группам устройств.

Модель групп пользователей —users_group (id, user's_access, user’s_rights).

В данном случае, user's_access показывает уровень доступа пользователя, относящегося к данной группе пользователей в определенные контролируемые зоны. В то время как user’s_rights показывает возможные действия пользователя, относящегося к данной группе пользователей (к ним относятся чтение, запись и удаление).

Модель групп устройств — comp_group (id, id_comp, id_zone).

Данная модель отражает принадлежность компьютера id_comp к контролируемой зоне id_zone. Эта модель также может быть расширена, в случае если вместо одного устройства id_comp будет стоять группа устройств.

Модель доступа групп пользователей в контролируемые зоны — zone_access (id, id_users_groups, id_zone).

Эта модель служит для демонстрации уровня доступа групп пользователей к контролируемым зонам.

Модель доступа групп пользователей к устройствам — comp_access (id, id_users_groups, id_comp).

Предложенная модель служит для отображения доступа группы пользователей к устройству.

Для двух вышеуказанных моделей целесообразно предусмотреть также более общие их варианты, которые включают в себя группу контролируемых зон в первом случае и группу устройств — во втором.

Модель принадлежности пользователей к группам пользователей— user_belongs_to_group (id, id_user, id_users_group).

Данное отношение показывает, что пользователь id_user имеет доступ в контролируемые зоны и доступ к устройствам, предложенный проектировщиками информационной системы для группы пользователей id_users_group.

Модель принадлежности технических устройств к группам устройств—comp_belongs_to_group (id, id_comp, id_comp_group).

Данное отношение показывает, что устройство id_comp входит в группу устройств id_comp_group.

4.Реляционная модель для построения топологии сети. Для того чтобы построить топологию сети анализируемой информационной системы, была введена реляционная модель, отображающая связи устройств между собой. Предложенное задание связи предусматривает

ее направленность. Но также возможно рассматривать ненаправленные связи. Описание данной модели приведено ниже — link (id, id_comp_x, id_comp_y). В данном случае id— это ключ базы данных для организации доступа к данной связи, id_comp_x— первое из устройств, между которыми установлена связь, а id_comp_y— второе.

5.Реляционная модель для построения связей между пользователями. Данная модель представляет собой модель relation (id, type_of_relation, user1, user2). В данном случае, если рассматривать варианты связей более тщательно, type_of_relation может принимать значения, например, из множества {friend, chief, subordinate, colleague, business, commoninterest, passion}. Кроме того, существенным является то, к какому множеству документов имеет доступ тот или иной пользователь. Имея указанные выше сведения, можно предположить, какие именно противоправные действия может совершить пользователь по отношению к критичным документам. Множеством таких действий может быть, например, {bargain, open, borrow, transfer, letuse}. Кроме того, можно указать ряд условий, при которых данные противоправные действия могут быть совершены, например — {продажа своих идентификационных данных, продажа доступных документов, продажа своих прав доступа в контролируемые зоны, продажа модулей хранения информации}.

6.Реляционные модели уязвимостей пользователя. Предполагается, что склонность пользователя совершать те или иные действия (либо не совершать таковые) в ответ на атакующие действия злоумышленника, характеризуется профилем уязвимостей пользователя [2, 3]. Например, фрагмент такового профиля уязвимостей может выглядеть следующим образом [1–3]. Реляционная модель состоит из множеств уязвимостей пользователя, множеств элементарных атакующих воздействий злоумышленника на данные уязвимости пользователя, а также из множества ответных действий пользователя. Таким образом, получается модель следующего вида —vulnerability (id, vulnerability, intruder_action, user_action). В данной модели представленные аргументы имеют следующую трактовку: id— это ключ базы данных для организации доступа к данной уязвимости, vulnerability — название уязвимости пользователя, intruder_action — элементарное атакующее воздействие злоумышленника, которое может быть применено к данной уязвимости, user_action — действие пользователя в ответ на данное атакующее воздействие пользователя.

Стоит отметить, что действия пользователя тесно связаны с теми правами, которые пользователь имеет на том или ином устройстве.

Также существенные сведения формализует модель для представления распределения вероятностей успешного завершения действия злоумышленника —intruder_success (id, id_vulnerability, id_uservulnerability_rate, intruder's_action, p_success). В данной модели представленные аргументы трактуются следующим образом: id— это ключ базы данных для организации доступа к данному распределению вероятностей, id_vulnerability — идентификационный номер уязвимости, на которую совершается атака злоумышленника, id_uservulnerability_rate — степень выраженности данной уязвимости у конкретного пользователя, intruder's_action — элементарное атакующее воздействие злоумышленника, p_success — вероятность успешного завершения атакующего воздействия злоумышленника на данную уязвимость пользователя, с учетом того, что степень выраженности данной уязвимости составляет id_uservulnerability_rate.

В данном случае рассматривается успех атакующего воздействия злоумышленника intruder's_action на уязвимость id_vulnerability при степени выраженности данной уязвимости у пользователя, равной id_user_vulnerability_rate. Успешность атакующего воздействия злоумышленника в данном случае имеет вероятностную оценку и выражается через p_success. В упрощенной модели, которая рассматривается в данной статье ниже, принято допущение о наличии 4 возможных значений вероятности успеха атакующего действия по каждой уязвимости. Такая градация возможных значений обусловлена разделением шкалы, отображающей степень выраженности уязвимостей пользователя, квартилями. Таким образом, достигается существенное упрощение вычисления вероятностных оценок, вместе с тем переход к более обобщенной модели вычисления вероятностных оценок не представляет существенных затруднений.

7. Пример применения моделей, основанных на отношениях, к SQL-представлению контекста социо-инженерной атаки и ее реализации. Рассмотрим информационную систему, описанную реляционными моделями, приведенными выше, и построим социо-инженерную атаку на персонал информационной системы. Комплекс «информационная система – персонал – критичные документы» представлен таблицами в СУБД, между которыми установлены связи. Реализация такой информационной системы представлена на рис.1.

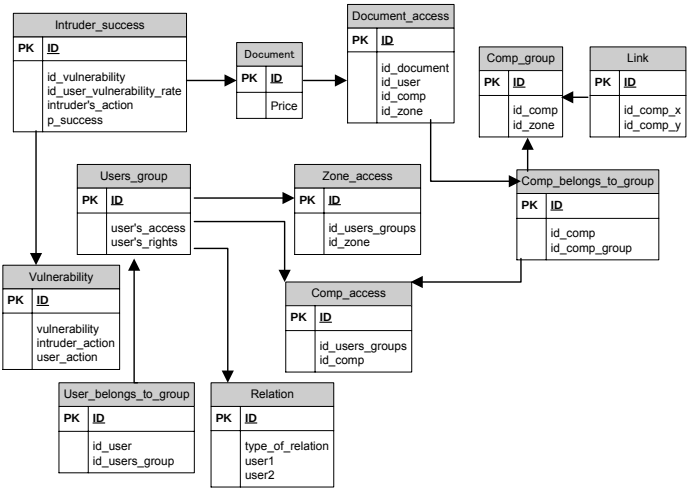

Рис.1. Представление связей между реляционными таблицами

Рассмотрим пример социо-инженерной атаки на персонал информационной системы. Данная информационная система представлена на Рис.2.

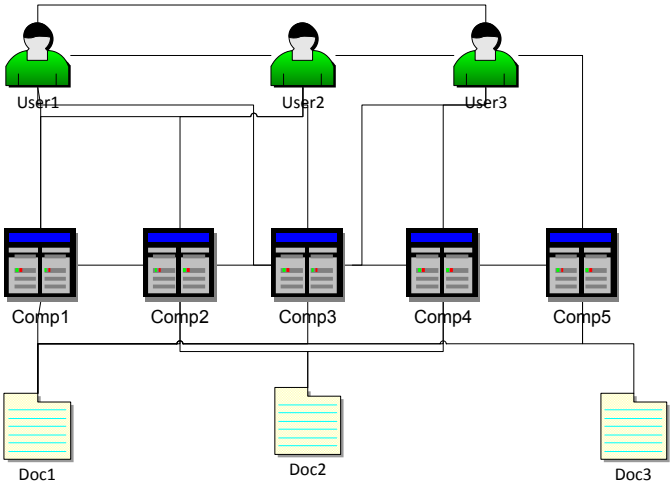

Рис. 2. Иллюстративный пример комплекса «персонал – информационная система – критические документы».

Для этого зададим наполнение представленной выше базы данных. Пусть у нас есть 3 пользователя информационной системы: $USER_1$, $USER_2$, $USER_3$. $USER_1$ является наиболее уязвимым пользователем (имеет максимальные значения уязвимостей). $USER_2$ имеет средние значения уязвимостей, а $USER_3$ является наиболее защищенным пользователем. Также система содержит 5 устройств: $COMP_1$, $COMP_2$, $COMP_3$, $COMP_4$, $COMP_5$. На каждом из них хранится критичная информация. Таких документов 3: DOC_1, DOC_2, DOC_3. Документ DOC_1 имеет наименьшую критичность и содержится на всех устройствах информационной системы. Документ DOC_2 имеет среднюю критичность и содержится на устройствах $COMP_2$ и $COMP_4$. Документ DOC_3 имеет наивысшую критичность и содержится на устройстве $COMP_5$. Пользователь $USER_1$ имеет доступ к устройствам $COMP_1$, $COMP_3$. Пользователь $USER_2$ имеет доступ к устройствам $COMP_1$, $COMP_2$, $COMP_3$. А пользователь $USER_3$ имеет доступ к устройства $COMP_3$, $COMP_4$, $COMP_5$. Между пользователями $USER_1$ и $USER_2$ существует связь «коллеги». Пользователь $USER_3$ является начальником, что означает, что есть связь «подчиненные». Злоумышленник обладает 100 условных единиц ресурса для воздействия на пользователей. Пользователь $USER_1$ требует 45 ресурсов для того чтобы оказать помощь злоумышленнику, $USER_2$ – 55, а $USER_3$ – 105.

Пусть злоумышленнику требуется документ DOC_2. Злоумышленник совершает элементарное атакующее воздействие на пользователя $USER_1$. Пользователь проверяет наличие требуемого злоумышленнику документа на устройствах, к которым у него есть доступ. Данного документа не было обнаружено. Поэтому пользователь $USER_1$ использует связь с пользователем $USER_2$. За свои услуги пользователь $USER_2$ требует ресурс. Злоумышленник отдает пользователю $USER_2$ требуемые ресурсы. $USER_2$ проверяет наличие документа на доступных ему устройствах. Документ найден и передан злоумышленнику. Атака завершена успешно, защищенность системы неудовлетворительна.

Разработанное SQL-представление моделей злоумышленника и комплекса «персонал – информационная система – критические документы» при реализации в реляционной СУБД и после наполнения БД соответствующими данными позволяет сводить различные задачи, возникающие при оценке защищенности персонала информационной системы от социо-инженерных атак, к выполнению соответствующих SQL-запросов.

В качестве примера, иллюстрирующего полученный основной результат настоящей работы, приведем SQL-запрос, который может быть использован для выявления пользователя, с помощью которого может быть успешно совершена социо-инженерная атака, а также при каких условиях и с какой целью.

```
SELECT *
FROM Intruder_success, Document, Document_access,
Comp_access, User_group, Relation
WHERE
Intrudersuccess.psuccess > 0.75 &&
Document_access.id_comp ==Comp_access.id_comp&&
User_group.user's_rights ==
Comp_access.id_comp&&Realtion = "colleague"
```

Также можно привести пример получения оценки вероятности успешности атакующего воздействия злоумышленника на пользователя.

```
SELECT Intrudersuccess.psuccess
FROM Intruder_success, Document, Document_access,
Comp_access, User_group
WHERE
Document.id == 1 &&
Document_access.id_comp ==Comp_access.id_comp&&
User_group.user's_rights == Comp_access.id_comp
```

8. Заключение. В данной статье рассмотрен подход к представлению реляционно-вероятностных моделей комплекса «персонал – информационная система – критические документы» с помощью SQL представления. Предложенный подход представляет реляционные модели, задающие автоматизированную информационную систему, а также пользователей данных систем. Хотя предложенные реляционные модели были ориентированы на реализацию в современных реляционных СУБД и использование преимуществ последних, стоит отметить, что может быть предложена их реализация в совершенно ином классе систем — продукционных систем, поддерживающих соответствующие виды вывода. Планируется, что предложенное в данной статье представление позволит существенно ускорить работу программного комплекса за счет применения аппаратно адаптированных операций, реализованных в современных реляционных СУБД.

Литература

1. *Азаров А.А., Тулупьева Т.В., Фильченков А.А., Тулупьев А.Л.* Вероятностно-реляционный подход к представлению модели комплекса «Информационная система – персонал – критичные документы». // Труды СПИИРАН. 2012. Вып. 20. С. 57–71.

2. *Азаров А.А., Тулупьева Т.В., Тулупьев А.Л.* Прототип комплекса программ для анализа защищенности персонала информационных систем построенный на основе фрагмента профиля уязвимостей пользователя. // Труды СПИИРАН. 2012. Вып. 21. С. 21–40.

3. *Ванюшичева О.Ю.* Прототип комплекса программ для построения профиля психологически обусловленных уязвимостей пользователя. 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. *Юсупов Р., Пальчун Б.П.* Безопасность компьютерной инфосферы систем критических приложений. Вооружение. Политика. Конверсия. 2003. № 2. С. 52.

22. *Dorothy D.E.* A Lattice Model of Secure Information Flow // Communications of the ACM. 2008. Vol. 19.No. 5. p. 236–243.

23. *Balepin I., Maltsev S., Rowe, J., Levitt K.* Using specification-based intrusion detection for automated response //Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection. 2003. p. 135-154.

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

25. National Institute of Standards and Technology. URL: http://www.nist.gov/index.html (дата обращения 24.06.2012)

26. Siemens. The total information security toolkit. URL: http://www.cramm.com/(дата обращения 24.06.2012)

27. Software Engineering Institute. URL: http://www.cert.org/octave/ (дата обращения 24.06.2012)

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

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

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

Tulupyev Alexander Lvovich — Dr. Sc. in Physics and Mathematics, associate professor; head of Laboratory of Theoretical and Interdisciplinary Computer Science, SPIIRAS, associate professor, Computer Science Department, Faculty of Mathematics and Mechanics, SPbSU. Research interests: uncertain knowledge and data representation and processing, application of mathematics and computer science in socio cultural and epidemiological studies, software technologies and development of information systems with databases. The number of publications — 200. ALT@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14-thLine V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

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

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

Поддержка исследований. Исследование поддержано грантом РФФИ на 2010–2012 гг., проект № **10-01-00640-а**, грантом СПбГУ на 2011–2013 гг., проект № **6.38.72.2011**.

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., Тулупьев А.Л., Тулупьева Т.В. **SQL-представление реляционно-вероятностных моделей социо-инженерных атак в задачах расчета агрегированных оценок защищенности персонала информационной системы.**

Анализ рисков информационной безопасности в настоящее время является особо актуальной темой в силу того, что и страховые компании хотят иметь возможно более точные характеристики о вероятном размере ущерба и необходимой сумме страхования, и компании, желающие застраховать свои информационные риски, также хотят понимать, за что именно и насколько обоснованно платятся те или иные суммы при заключении договора страхования. Кроме того, ни одна из названных сторон не хочет терять собственные ресурсы. Таким образом, необходимо научиться получать адекватные, но в то же время комплексные, агрегированные оценки защищенности информационных систем. Для этого необходим всесторонний анализ защищенности как программно-технической составляющей системы, так и персонала таких систем (их социотехнической составляющей). Настоящая работа концентрируется на возможном подходе к автоматизации анализа защищенности пользователей информационных систем от социо-инженерных атак. Социо-инженерная атака рассматривается как реализация элементарных атакующих действий, направленных на уязвимости пользователя. Данный подход был рассмотрен в статьях. Для разработки модели, а затем — подходящих структур данных, для реализации алгоритмов автоматизированного анализа защищенности от социо-инженерных атак было решено применить реляционно-алгебраический подход. Он позволяет, с одной стороны, перейти к отношениям для представления данных, то есть для представления модели контекста, в котором будут развиваться социо-инженерные атаки, и модели злоумышленника, и, с другой стороны, использовать эффективные алгоритмы обработки SQL-запросов, реализованные в современных СУБД, для вычисления искомых показателей — агрегированных оценок степени защищенности персонала, либо степени «поражаемости» критичных документов при социо-инженерных атаках.

Целью настоящей статьи является рассмотрение варианта задания основных отношений в комплексе «персонал - информационная система – критичные документы» при социо-инженерной атаке злоумышленника, а затем иллюстрация работы принципов вероятностно-реляционного подхода на упрощенном (для доступности и краткости изложения) примере. Будем использовать смешанную терминологию, заимствованную из теории отношений и теории реляционных БД.

SUMMARY

Azarov A.A., Tulupyev A.L., Tulupyeva T.V. **SQL representation of relational and probabilistic models of socio-engineering attacks in problems of calculation of the aggregated of information system's personnel's security estimation.**

Risk analysis of information security nowadays is an extremely important topic, due to the fact that insurance companies want to have probably more exact characteristics about the probable size of a damage and the necessary sum of insurance, and the company, wishing to insure the information risks, also wants to understand, for what it does pay at the conclusion of the contract of insurance and if these fees are reasonable. Besides, both mentioned above parties don't want to lose their resources. The all-round analysis of security both of a program and technical component of system, and the personnel of such systems (their sociotechnical component) is for this purpose necessary. The real work concentrates on a possible approach to automation of the analysis of security of users of information systems from socio-engineering attacks. Socio-engineering attack is considered as realization of elementary attacking actions on vulnerabilities of the user and reciprocal actions of the user. This approach was considered in different papers. It was decided to apply a relational and algebraic approach for the developing of models, and then — suitable structures of data, and realization of algorithms of the automated analysis of security from socio-engineering attacks. It will allow to pass, on the one hand, to the relations for data presentation, that is for representation of model of a context in which socio-engineering attacks will develop, and models of the malefactor, and, on the other hand, to use effective algorithms of processing of the SQL inquiries, realized in modern DBMS, for calculation of required indicators — the aggregated estimates of degree of security of the personnel or degree of "susceptibility" of critical documents at socio-engineering attacks.

The purpose of the present article is consideration of setting of general relations in a complex «the personnel information system – critical documents» at socio-engineering attack of the malefactor, and then illustration of work of principles of a likelihood and relational approach on simplified (for availability and brevity of a statement) example. We'll use the mixed terminology borrowed from the theory of the relations and the theory of relational DB.