УДК 614.8+002.6:004.89

А.Л. Тулупьев, А.Е. Пащенко, А.А. Азаров

ИНФОРМАЦИОННАЯ МОДЕЛЬ ПОЛЬЗОВАТЕЛЯ, НАХОДЯЩЕГОСЯ ПОД УГРОЗОЙ СОЦИОИНЖЕНЕРНОЙ АТАКИ

Тулупьев А.Л., Пащенко А.Е., Азаров А.А. **Информационная модель пользователя, находящегося под угрозой социоинженерной атаки.**

Аннотация. Статья посвящена развернутому описанию информационной модели пользователя, находящегося под угрозой социоинженерной атаки, и ряду других моделей, связанных с упомянутой: групп пользователей, контролируемых зон, информационных объектов (документов). Указанные информационные модели входят в состав базы для анализа защищенности персонала информационной системы от социоинженерных атак. Информационная модель пользователя позволяет учитывать имя и фамилию пользователя, его должность в организации, принадлежность пользователя к группам, а также уязвимости пользователя перед социоинженерными атаками. Информационная модель групп пользователей позволяет учитывать название такой группы, ее описание, разрешение тех или иных атомарных действий, которые пользователи могут выполнять с информационными объектами, тип доступа к информационным объектам этой группы, а также информационные объекты, к которым имеет доступ данная группа пользователей. Информационная модель контролируемой зоны позволяет учитывать название контролируемой зоны и ее описание. Информационная модель информационного объекта позволяет учитывать оценки ущерба при потере конфиденциальности, целостности, а также достаточности. Приведен пример социоинженерной атаки, развитие которой описано с использованием предложенных информационных моделей.

Ключевые слова: информационная модель, пользователь, информационная система, социоинженерная атака, злоумышленник.

Tulupyev A.L., Paschenko A.E., Azarov A.A. **Information model of the user, who may be under the threat of socioengineering attack.**

Abstract. This paper is devoted to developed description of informative model of the user, who may be under the threat of socioengineering attack, and some other models, which is connected to the first one: users group model, model of control area, informative objects (documents) model. Specified informative model are included into the base for analyzing of the protection of users of informative system from socioengineering attack. Informative model of the user allows to consider name and surname of the user, his post in the organization, belongings of user to user group, and vulnerability of the user on socioengineering attacks. informative model of user group allows to consider name of user group, it's description, allows for different atomic actions which user can perform with informative objects, type of access to information objects and information objects, which this group of users can use. Informative model of control area allows to consider name of control area and it's description. Information model of information objects includes damage estimation of losses of confidentially, losses of integrity and losses of sufficiency. The example of socioengineering attack is brought. Development of this attack is described through suggested informative models.

Keywords: informative model, user, informative system, socioengineering attack, malefactor.

1. Введение. Чтобы оценить степень защищенности комплекса «информационная система—персонал» от социоинженерных атак, следуя подходу, представленному в [7], необходимо осуществить перебор

всех возможных реализаций атак такого рода. (Вопросы оптимизации перебора представляются справедливыми, но их рассмотрение будет отложено до достаточно полной формализации задачи.) Возможные реализации атаки имитируются с помощью последовательностей атакующих действий, причем сведения о таких последовательностях впоследствии организуются в виде особой структуры, получившей название «деревьев атак» (и в более общей ситуации — графов атак). Имитация атаки осуществляется в рамках некоторой сцены или контекста, которые отражают состояния комплекса «информационная система—персонал» и их изменения в ответ на атакующие действия [10, 11].

Чтобы сымитировать процесс атаки на компьютере (а затем, используя этот процесс как инструмент перебора, построить дерево атак для последующего анализа степени защищенности комплекса), требуется разработать информационную модель, описывающую сцену (контекст) осуществления атаки. А после того, как модель будет разработана, ей потребуется сопоставить представление данных, с помощью которого информационная модель будет реализована в комплексе компьютерных программ.

Информационная модель сцены (контекста) действия социоинженерной атаки состоит из ряда компонент-«подмоделей». Среди них выделим основные, которые отвечают за описание следующих элементов:

— набора документов, хранящихся в информационной системе и характеризующихся различной степенью критичности по отношению к раскрытию, утрате и изменению;

— набора программно-технических компонент информационной системы;

— коллектива пользователей;

— связей между вышеуказанными компонентами.

Кроме того, стоит упомянуть отдельно информационную модель злоумышленника и его связей с компонентами комплекса, подвергающегося социоинженерной атаке. Некоторые информационные модели из упомянутых также допускают декомпозицию на «подмодели», так что, в конечном счете, в целях достаточной полноты и строгости формализации описания комплекса «информационная система—персонал» потребуется разработать иерархию информационных моделей.

В настоящей работе нас интересует развитие информационной модели пользователя, как непосредственного объекта социоинженерной атаки. Ряд требований к такой модели предъявлен в [8]. Кроме того, в цели исследования входит разработка основных элементов представления данных, ориентированного на использование получен-

ной модели в программной реализации, а также иллюстрация ее возможного использования при имитации атаки.

2. Информационная модель пользователя. Информация о пользователе не сводится к перечислению таких формальных атрибутов, как имя, фамилия и должность, хотя, безусловно, последний атрибут может содержать критичные данные, существенные для анализа степени защищенности. В первую очередь информационная модель пользователя должна обеспечивать описание его уязвимости в отношении социоинженерных атак [9]. Поэтому кроме указанного набора преимущественно идентифицирующих данных в характеристику пользователя необходимо включить еще несколько параметров, разбивающихся на две группы:

1) права доступа данного пользователя;
2) наличие и степень проявления уязвимостей.

Права доступа пользователя делятся на две подкатегории:

1) доступа в помещения (так называемые «зоны доступа»),

2) доступа к устройствам (зачастую характеризующиеся набором политик доступа).

Таким образом задаются ограничения на нахождение пользователя в определенных помещениях компании. Например, никому из сотрудников компании может быть не разрешено находится в кабинете директора, если самого директора там нет.

Кроме того, у пользователей есть ограниченные права доступа к компьютерам. Существуют учетные записи, которые предоставляют пользователям определенные права и соразмерные с ними действия. Следует учитывать, что пользователи могут составлять группы пользователей, участники которых обладают одинаковыми правами.

Декомпозиция коллектива пользователей на группы обладает потенциалом по снижению вычислительной сложности последующего анализа степени защищенности комплекса «информационная система—персонал», поскольку ожидается, что в ряде случаев перебор атакующих действий в отношении каждого пользователя можно останавливать, если последовательность таких действий привела к успеху в отношении хотя бы одного представителя соответствующей группы пользователей.

Уязвимость пользователей перед социоинженерными атаками — это целая система факторов, среди которых в качестве наиболее критичных предлагается выделить следующие [1]:

1) возможность подкупа пользователя;
2) возможность шантажа пользователя;
3) социальные и личностные проблемы пользователя;
4) желание пользователя самовыразиться (нарциссизм).

Заметим, что список факторов, характеризующих уязвимости, можно пополнить (и, скорее всего, он пополнится при переходе к прикладной фазе исследований), однако для развития метода, принципов моделировании и алгоритмов имитации социоинженерных атак указанного списка достаточно [6]. Не ожидается, что его пополнение приведет к появлению существенно новых алгоритмов перебора, лежащих в основе анализа степени защищенности комплекса, хотя сам перебор, скорее всего, станет более трудоемким.

В отличие от детерминированных систем, реакции пользователя на внешнее воздействие (в контексте настоящей статьи — на атаку) однозначно не определены. Неопределенность такого рода предлагается учитывать, используя распределение вероятностей, характеризующих ту или иную ответную реакцию (или их совокупность) пользователя. Например, пользователь удовлетворен своей зарплатой, у него нет никаких материальных проблем, тогда вероятность того, что его можно будет подкупить, будет нулевой или близкой к нулю. Если же пользователь доволен своей заработной платой, однако у него неожиданно возникли материальные проблемы, которые сам он решить не может, но при этом велика его преданность фирме, успешность реализации подкупа может возрасти до 33 %.

Разумеется, численные оценки такого рода параметров требуют широкого спектра прикладных исследований в науках, объектом исследования которых выступает поведение; кроме того, указанный параметр может иметь функциональную зависимость от контекста, в котором осуществляется атака, и особенностей злоумышленника, ее осуществляющего. На данном этапе исследования излишне глубокая детализация отношений представляется неоправданной; мы не станем усложнять выбор оценок вероятностей, что, тем не менее, не помешает продемонстрировать позже все принципиально важные моменты развиваемого подхода.

Развитие информационной модели пользователя невозможно без упоминания других моделей из упомянутой выше иерархии; они привлекаются к обсуждению по мере необходимости.

3. Основные требования к сопутствующим информационным моделям. В первую очередь необходимо принять в рассмотрение модель групп пользователей. Эта модель служит для объединения пользователей в группы с одинаковыми правами на работу с техническими устройствами; в частности, участники каждой такой группы имеют одинаковые права на одинаковые атомарные действия, которые они могут применять по отношению к файлам на заданных устройствах.

Формирование модели зон доступа также является неизбежным шагом, который может существенно сказаться и на самой защищенно-

сти комплекса «информационная система—персонал», и на подходе к анализу указанной защищенности [2]. Предполагается, что сначала определяются несколько контрольных зон, чтобы затем распределить по ним пользователей и устройства. При этом пользователи, имеющие доступ к различным контрольным зонам, могут относиться к одинаковым группам, т.е. при обладании одинаковыми правами в отношении политик доступа они могут различаться в окончательном наборе возможностей осуществить операции чтения, модификации (вплоть до подмены) и удаления элементов из набора критичных документов.

Анализа защищенности также требует информационная модель указанного набора критичных документов (более обще — набора критичных информационных объектов) [3], в который входят сведения о следующем:

— составе набора документов;

— критичности ряда операций с каждым документом;

— какие пользователи к какой части набора в какой степени имеют доступ.

Для этого вводится модель документа (информационного объекта), обладающая рядом атрибутов, среди которых в качестве основных можно выделить

1) идентификационные данные объекта;
2) оценку ущерба при потере конфиденциальности;
3) оценку ущерба при потере целостности;
4) оценку ущерба при потере достаточности.

Последние три атрибута позволяют в свою очередь вывести оценку критичности документа (информационного объекта, файла) для данного комплекса «информационная система—персонал» и оценку ущерба организации, который возникает при несанкционированной операции с документом [4]. С точки зрения реализации основных принципов подхода к анализу защищенности комплекса от социоинженерных атак и во избежание высокой трудоемкости предварительных вычислительных экспериментов, представляется достаточным соотносить файлы, в которых хранятся документы, с группами пользователей. Это упрощение представляется весьма реалистичным, поскольку зачастую компьютеры информационной системы объединены в сеть и доступ к данным администрируется так, что к файлам, в которых хранятся критичные документы, имеется доступ с любого компьютера в сети.

Уже на основе требований, предъявленных к рассмотренным информационным моделям (перечень которых далеко не полон и содержит только ключевые для понимания и развития предлагаемого подхода

элементы), можно предложить проект структуры базы данных, обеспечивающей хранение сведений о сценах (контексте), в которых могут развиваться социоинженерные атаки. Такая база данных — важная составляющая для анализа защищенности комплекса «информационная система—персонал» от социоинженерных атак; однако в зависимости от степени детальности и конкретной цели анализа может также потребоваться другая база данных, которая содержит сведения о программно-технических компонентах системы, об их связях и уязвимостях.

4. База данных для представления иерархии информационных моделей, связанных с коллективом пользователей и набором критичных документов. Переходя к представлению перечисленных информационных моделей в комплексе программ, получаем проект структуры базы данных, которая состоит из четырех основных таблиц: 1) «Пользователи», 2) «Группы пользователей», 3) «Информационные объекты» и 4) «Контрольные зоны», а также одной таблицы-связки «Пользователи—Контрольные зоны». (Информационные объекты в настоящем разделе используются как синоним набора критичных документов.)

Таблица «Пользователи» содержит следующие поля:

— ID пользователя,
— имя пользователя,
— фамилия пользователя,
— должность,
— принадлежность к группе пользователей,
— возможность подкупа,
— возможность шантажа,
— наличие социальных и личностных проблем,
— наличие нарциссизма.

Таблица «Группы пользователей» состоит из следующих полей:

— ID группы пользователей,
— имя группы пользователей,
— описание группы пользователей,
— разрешение на атомарное действие «Чтение»,
— разрешение на атомарное действие «Запись»,
— разрешение на атомарное действие «Удаление»,
— тип доступа «Локальный»,
— тип доступа «Удаленный»,
— информационные объекты.

Таблица «Информационные объекты» имеет в своем составе следующие элементы:

— ID информационного объекта,
— имя файла,
— потери конфиденциальности,
— потери целостности,
— потери достаточности.

Таблица «Контролируемые зоны» содержит следующую информацию:

— ID контролируемой зоны,
— название контролируемой зоны,
— описание контролируемой зоны.

Таблица — связка между пользователями и контролируемыми зонами содержит следующие поля:

— ID связи,
— ID пользователя,
— название контролируемой зоны.

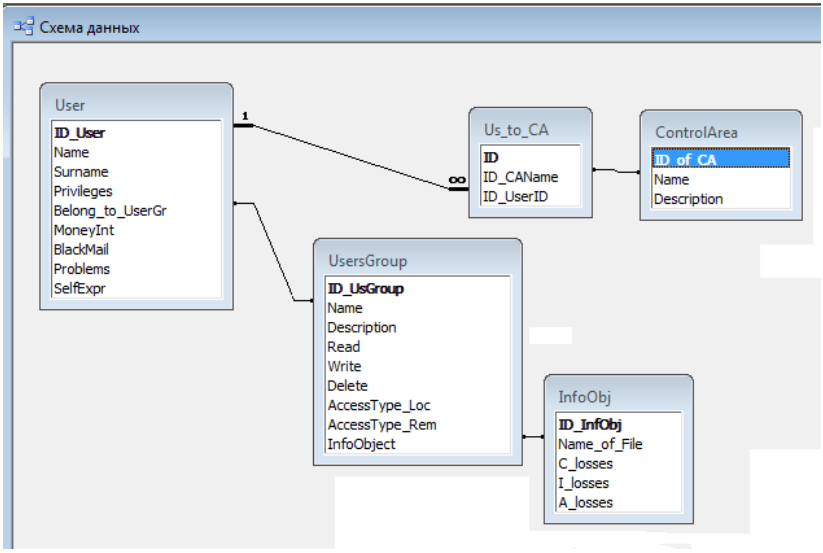

Схема базы данных.

На рисунке изображена схема базы данных, описанной в этой части статьи.

В целях иллюстрации того, как развитые информационные модели, реализованные в виде базы данных, могут быть использованы в

имитации социоинженерной атаки и далее в анализе степени защищенности комплекса «информационная система—персонал» от такого рода атак, в следующем разделе разбирается достаточно схематичный, но содержательный пример.

5. Пример реализации социоинженерной атаки. Будем считать, что злоумышленнику требуется какой-то информационный объект (документ), находящийся в системе. Злоумышленник пытается применить к пользователю социоинженерную атаку, начальный этап которой признается успешным, если пользователя удалось склонить к противоправным действиям, а в целом атака признается успешной, если злоумышленнику удалось получить тот информационный объект, который ему был нужен изначально [12]. Рассмотрим реализацию этой схемы на примере социоинженерной атаки, в которой используется такая уязвимость пользователя, как «возможность подкупа».

Рассмотрим ситуацию, когда атака осуществилась, т.е. пользователя оказалось возможным подкупить. Он получает информацию о том, какие данные ему надо найти и передать злоумышленнику, и начинает действовать [5].

В первую очередь пользователь проверяет те файлы, к которым имеет доступ группа пользователей, к которой он относится. В таком случае возможны две ситуации: нужный информационный объект 1) доступен или 2) недоступен. Проанализируем эти две возможности и рассмотрим действия при реализации каждой из них.

1. Доступ к искомой информации возможен. В таком случае пользователь может совершить следующие действия:

— отдать сетевой логин-пароль злоумышленнику (что позволяет извне получить доступ к искомой информации);

— скопировать информационный объект, необходимый злоумышленнику, и позже передать ему копию объекта.

2. Прямой доступ к искомой информации невозможен. В этом случае пользователь может совершить следующие действия:

а) попытается отсканировать информационную систему, чтобы выявить ее структуру, тем самым облегчая задачу злоумышленнику (см. пункт *в*);

б) пробует предположить (перебирая доступные варианты), где может находиться интересующая злоумышленника информация, и перейдет к пункту *г*;

в) попытается установить ПО, которое даст злоумышленнику удаленный доступ в информационную систему (предполагается, что злоумышленник провел удачную атаку на систему, тогда пользователь

свою функцию выполнил и далее злоумышленник работает автономно);

г) попытается подменить себя другим пользователем (т.е., переориентирует последующие атакующие действия на другого пользователя), предположительно из другой группы пользователей, и обеспечит его контакт (знакомство) со злоумышленником

Сотрудничество злоумышленника с пользователем продолжается до тех пор, пока не случится одно или сразу несколько следующих событий:

— атака злоумышленника достигла своей цели;

— пользователь исчерпал все свои связи;

— цена предоставления новой связи пользователем выше, чем имеющиеся остатки ресурсов у злоумышленника;

— пользователя вычисляет служба безопасности, а взаимодействие злоумышленника с этой службой считается невозможным (отметим, что это все же достаточно серьезное допущение).

6. Заключение. Предложенная схема развития социоинженерной атаки не исчерпывает все возможные действия и со стороны злоумышленника, и со стороны пользователя. Существуют другие возможности получения или повреждения информации пользователем, равно как и другие варианты атакующих действий. Однако основной принцип имитации атаки останется прежним: сначала идет перебор атакующих действий, затем изменяется позиция пользователя. Одновременно с этим пользователь может 1) изменить состояние информационной системы, 2) изменить состояние информационного объекта, 3) сообщить что-то злоумышленнику — все это изменяет контекст, в котором развивается атака. Наконец, злоумышленник либо получает доступ к нужному ему документу (информационному объекту), либо продолжает атаку в новом контексте, либо обнаруживает, что продолжать атаку невозможно.

Чтобы обеспечить имитацию отдельной социоинженерной атаки и на основе перебора всех возможных атак построить дерево атак, предназначенное для последующего вывода оценки степени защищенности комплекса «информационная система—персонал», необходимо использовать формальное описание контекста, в котором атака осуществляется. В статье предложена иерархия информационных моделей, включающая в себя пользователей, групп пользователей, информационных объектов (документов), контрольных зон и доступа пользователей в контрольные зоны. Указанным моделям сопоставлена структура реляционной базы данных.

Таким образом, построена информационная модель второй компоненты комплекса «информационная система—персонал», которую предстоит увязать с информационной моделью первой компоненты и злоумышленника.

Литература:

1. *Грановская Р.М., Крижанская Ю.С.* Творчество и преодоление стереотипов. СПб.: OMS, 1994. 180 с.
2. Котенко И. В., Степашкин М. В., Богданов В. С. Анализ защищенности компьютерных сетей на этапах проектирования и эксплуатации // Изв. вузов. Приборостроение. 2006. Т. 49, № 5. С. 3–8.
3. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 7–24.
4. Котенко И. В., Степашкин М. В. Использование ложных информационных систем для защиты информационных ресурсов компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2005. № 1. С. 63–73.
5. Котенко И. В., Степашкин М. В. Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Изв. вузов. Приборостроение. 2006. Т. 49, № 3. С. 3–8.
6. *Сапронов К.* Человеческий фактор и его роль в обеспечении информационной безопасности // [электронный ресурс *http://www.interface.ru/home.asp?artId=17137*].
7. *Степашкин М.В.* Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак: Дис… канд. техн. наук: СПб.: СПИИРАН, 2002. 196 с.
8. *Тулупьева Т.В., Тулупьев А.Л., Пащенко А.Е., Азаров А.А. и др.* Социально-психологические факторы, влияющие на степень уязвимости пользователей информационных систем, с точки зрения социоинженерных атак // Тр. СПИИРАН. 2010. Вып. 1(12).
9. *Тулупьева Т. В., Тулупьев А. Л., Пащенко А. Е., Степашкин М. В.* Подход к оценке защищенности персонала автоматизированной информационной системы от социоинженерных атак // Материалы XI Санкт-Петербургской междунар. конф. «Региональная информатика-2008 (РИ-2008)». Санкт-Петербург, 22–24 октября 2008 г. СПб., 2008. С. 113–114.
10. *Фролова А. Н., Тулупьева Т. В., Пащенко А. Е., Тулупьев А. Л.* Возможный подход к анализу защищенности информационных систем от социоинженерных атак // Тр. V Санкт-Петербургской региональн. конф. «Информационная безопасность регионов России (ИБРР-2007)». Санкт-Петербург, 23–25 октября 2007 г. СПб., 2008. С. 195–199.
11. *Фролова А. Н., Пащенко А. Е., Тулупьева Т. В., Тулупьев А. Л.* Анализ уровня защищенности информационных систем в контексте социоинженерных атак: постановка проблемы // Тр. СПИИРАН. 2008. Вып. 7. С. 170–176.
12. *Shaw E., Ruby K.G., Post J.M.* The Insider Threat to Information Systems The Psychology of the Dangerous Insider // Security Awareness Bulletin. 1998. N 2.

Тулупьев Александр Львович — д-р физ.-мат. наук, доцент; заведующий лабораторией теоретических и междисциплинарных проблем информатики (ТиМПИ) Учреждения Российской академии наук Санкт-Петербургского института информатики и автомати-

зации РАН (СПИИРАН), профессор кафедры информатики математико-механического факультета Санкт-Петербургского государственного университета (СПбГУ). Область научных интересов: представление и обработка данных и знаний с неопределенностью, применение методов математики и информатики в социокультурных исследованиях, применение методов биостатистики и математического моделирования в эпидемиологии, технология разработки программных комплексов с СУБД. Число научных публикаций — 210. ALT@iias.spb.su, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Tulupyev Alexander Lvovich — PhD in Appl. Math. and CS, Dr. Sci. in CS, associate professor; head of laboratory, Theoretical and Interdisciplinary Computer Science Laboratory (TICS Lab), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), professor, Computer Science Department, Faculty of Mathematics and Mechanics, St. Petersburg State University (SPbSU). Research interests: uncertain knowledge and data representation and processing, application of mathematics and computer science in sociocultural studies, applications of biostatistics and mathematical modeling in modern epidemiology, software technologies and development of information systems with databases. The number of publications — 210. ALT@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Пащенко Антон Евгеньевич — м. н. с. научно-исследовательской группы междисциплинарных проблем информатики Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: математическая статистика, статистическое моделирование, применение методов биостатистики и математического моделирования в эпидемиологии. Число научных публикаций — 35. AEP@iias.spb.su, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

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

Азаров Артур Александрович — студент математико-механического и экономического факультетов Санкт-Петербургского государственного университета. Область научных интересов: автоматизация анализа защищенности информационных систем с учетом социоинженерных атак. Число научных публикаций — 2. artur-azarov@yandex.ru, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Azarov Artur Alexandrovich — student of Saint-Petersburg State University of the faculties of Mathematics and Mechanics and Economics. Research interests: the analyzing protection of informative systems concerning socioengineering's attacks. The number of publications — 2. artur-azarov@yandex.ru, www.tulupyev.spb.ru; SPIIRAS, 39, 14th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

РЕФЕРАТ

Тулупьев А.Л., Пащенко А.Е., Азаров А.А. **Информационная модель пользователя, находящегося под угрозой социоинженерной атаки.**

Одним из основных вопросов развития анализа защищенности информационных систем становится анализ угроз с учетом человеческого фактора, т.е. с учетом реализации угрозы социоинженерных атак в отношении персонала таких систем. Современные системы защиты не всегда справляются с подобными угрозами.

Большинство продуктов, предназначенных для анализа защищенности информационных систем, не учитывает тот факт, что система может быть атакована изнутри компании ее сотрудниками. Поэтому результат, полученный при анализе систем таким продуктом, не всегда адекватно представляет уровень защищенности информационной системы.

При анализе защищенности информационной системы необходимо учитывать человеческий фактор. В статье рассматривается информационная модель пользователя, которая тесно связана с другими информационными моделями: групп пользователей, контролируемых зон и информационных объектов (документов). Эти модели предназначены для использования в инструментах автоматизированного анализа защищенности. В статье приведено описание свойств, которыми эти модели должны обладать, чтобы их можно было применять при оценке защищенности информационной системы, персонал которой они характеризуют. Совокупность информационных моделей позволяет строить сцену (контекст), в котором развивается (имитируется) социоинженерная атака. Впоследствии, за счет перебора всех возможных атак, могут быть рассчитаны различные оценки защищенности персонала информационной системы.

Рассмотрен пример работы части программного комплекса, предназначенного для имитации социоинженерных атак на основе описанной в статье совокупности информационных моделей, связанных с информационной моделью пользователя. Указанный пример иллюстрирует разработанную концепцию анализа защищенности персонала информационной системы.

Социоинженерные атаки не исчерпывают все возможные угрозы в отношении безопасности информационной системы. Для более полной оценки необходимо объединить текущий подход к оценке защищенности информационной системы, с учетом угроз социоинженерных атак, и подход к анализу технической составляющей информационной системы. В связи с эти впоследствии концепция будет расширена за счет использования других информационных моделей, необходимость которых может быть выявлена в дальнейшей работе с этой тематикой, а также за счет анализа технической составляющей системы.

SUMMARY

Tulupyev A.L., Paschenko A.E., Azarov A.A. **Information model of the user, who may be under the threat of socioengineering attack.**

One of the main questions in development of analyzing protection of informative system becomes analyzing threats of human factor, in other words taking into account realization of the threat of socio-engineering attack against personnel of such systems. Modern protection system does not deal successfully with such threats usually.

Main part of products, which analyzes protection of informative system, does not consider the fact that attack to the system may occur inside the company by its personnel. That is why the results, gained from analyzing systems by this product, does not represent the level of protection of informative system.

During analyzing protection information system it is essential to include human factor. The paper deals with informative model of the user, which is closely connected with some other informative models: user's group model, control area model and model of informative objects (documents). These models are used for automatic analyzing of protection. In the paper brought description of properties, which these models have to possess for being applied for estimating protection of informative system, the personnel of which they represent. Set of informative models allows to build scene (context) in which socio-engineering attack develops (imitated). Subsequently, at the expense of search of all possible attacks, all estimates of protection personnel of informative system may be calculated.

Example of work of part of program complex is examined in this paper. This complex is intended for imitation of socio-engineering attack, based on the set of informative models described in this article, and connected to the informative model of the user. This example illustrates developed conception of analyzing protection of personnel of informative system.

Socio-engineering attacks do not exhaust all threats to protection of informative systems which can occur. For more complicated estimation it is necessary to unite current method of estimating protection of informative system and method of analyzing technical part of informative system. Taking all this into account the concept will be expanded through using other informative models, the necessity of which can be occurred form further research of this topic, and though analyzing technical part of the system.