УДК 614.8+002.6:004.89

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

ИНФОРМАЦИОННЫЕ МОДЕЛИ КОМПОНЕНТ КОМПЛЕКСА «ИНФОРМАЦИОННАЯ СИСТЕМА—ПЕРСОНАЛ», НАХОДЯЩЕГОСЯ ПОД УГРОЗОЙ СОЦИОИНЖЕНЕРНЫХ АТАК

Тулупьев А.Л., Пащенко А.Е., Азаров А.А. **Информационные модели компонент комплекса «информационная система—персонал», находящегося под угрозой социоинженерных атак.**

Аннотация. Представлено развернутое описание информационных моделей компонент комплекса «информационная система—персонал», находящегося под угрозой социоинженерный атак. Рассмотрены информационные модели пользователя, групп пользователей, контролируемых зон, информационных объектов (систем документов), программно-аппаратного обеспечения и самой информационной системы. Указанные информационные модели входят в состав базы для анализа защищенности информационной системы при угрозах социоинженерных атак. Иерархия этих моделей позволяет описать сцену (контекст), в которой развивается социоинженерная атака, перебрать возможные атаки (деревья атак) и на основе полученных результатов изучить возможные подходы к оценке степени защищенности комплекса «информационная система—персонал» от социоинженерных атак.

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

Tulupyev A.L., Paschenko A.E., Azarov A.A. **Information models of the components of complex "information system—personnel", which is under threat of socioengineering attack.**

Abstract. Developed description of informative models of the component of complex "information system—personnel", which is under threat of socioengineering attack is being presented in this paper. Informative model of user, users group, controlling areas, information objects (system of documents), hardware-software maintenance and information system itself are considered. Specified informative models are included into the base for analyzing protection of informative system under the threat of socioengineering attacks. Hierarchy of these models allows to describe scene (context), in which socioengineering attack developes, to touch possible attacks (trees of attacks), and, on the base of gained results, study possible approaches to estimation the degree of protection of complex "information system—personnel" from socioengineering attack.

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

1. Введение. Большинство современных продуктов, нацеленных на анализ защищенности информационных систем, производит оценку лишь программно-аппаратной подсистемы, не учитывая уязвимостей персонала, который работает с ней. Соответственно остается открытым вопрос о коррекции оценок, полученных такими продуктами, таким образом, чтобы в них учитывалось влияние человеческого факто-

ра, находящегося под угрозой социоинженерных атак или, в некоторых случаях, самого по себе содержащего угрозу.

Указанный фактор является существенным. Например, информационная система может использовать все самые современные способы защиты, но если в нее на стадии разработки ведущим программистом была заложена логическая бомба, которую он может активировать в случае своего увольнения, то данная информационная система имеет серьезные пробелы в защите [11].

Цель настоящей работы — описать совокупность основных требований к информационным моделям компонент комплекса «информационная система—персонал». Указанные модели предназначены для представления сцены (контекстов), в которых будут имитироваться социоинженерные атаки, направленные против персонала информационных систем.

Описание информационных моделей, связанных с представлением персонала основывается на требованиях, сформулированных в [7–8]. Требования и подходы к формированию информационных моделей программно-технической составляющей информационной системы основываются на работах [1–5, 9–12].

2. Составляющие информационной системы. В статье [8] рассмотрены информационные объекты (документы), которые по умолчанию относились к каким-то устройствам, но не было конкретизации того, к каким именно. В связи с этим информационная система в первую очередь будет расширена за счет устройств, которые присутствуют в системе [5]:

— ПК и периферийных устройств, таких как принтеры;

— сетевых адаптеров для ПК и сетевых кабелей;

— сетевого оборудования, такого как концентраторы и коммутаторы, которые соединяют между собой ПК и принтеры;

— сетевой операционной системы, например Windows NT или NetWare.

Каждому из этих устройств соответствуют какие-то информационные объекты, которые хранятся на этих устройствах. Критичными свойствами для устройств, которые в будущем помогут оценить защищенность информационной системы по технической базе, являются их программно-технические составляющие.

Кроме того, каждое устройство может быть отнесено к определенной контролируемой зоне (информационной модели, рассмотренной в статье [8]). Например, с одной стороны, компьютер младшего менеджера по продажам в какой-либо компании, вероятнее всего, не

имеет никакой защиты, которая связана с отнесением его к контролируемой зоне [11]. С другой стороны, к компьютеру старшего менеджера этой же компании имеет доступ только он лично, потому что, как правило, у сотрудников с подобным статусом есть свой кабинет.

Чтобы оценивать защищенность системы по технической базе, необходимо также знать, какие связи существуют между устройствами. Но, несмотря на важность этого параметра, он может не влиять на защищенность системы. Так, например, если информационная система состоит из нескольких групп обособленных устройств, и мы рассматриваем атаку на одну из этих групп, но искомая информация хранится в другой группе, то обычный программный комплекс, анализирующий защищенность системы, укажет, что система защищена. Однако если мы присовокупим персонал к этой системе, то может оказаться, что какой-то сотрудник имеет доступ как к обеим группам и может получить информацию из любой из них. Тогда защищенность системы уже неудовлетворительна. Поэтому в информационную систему необходимо добавить также и связи между пользователями и устройствами.

И последней информационной моделью станет сама информационная система. Это необходимо, чтобы отнести все устройства, пользователей, группы пользователей к определенной информационной системе, а также, чтобы получить о ней общие сведения.

3. Персонал информационной системы.

В статье [8] сведения о персонале информационной системы также представляются посредством информационных моделей. Пользователям системы сопоставляется информационная модель, которая содержит важнейшие свойства (атрибуты) пользователей. Эти свойства разбиты на три смысловые группы:

1) общая информация о пользователе,
2) информация о правах пользователя в информационной системе,
3) наличие (степень проявления) уязвимостей у пользователя.

Таким образом, учет указанных свойств позволяет не только дать в какой-то мере исчерпывающую информацию для анализа степени защищенности информационной системы с учетом риска социоинженерных атак, но и упростить этот анализ за счет явного указания уязвимостей пользователя. Заметим, что один из подходов к упрощению состоит в том, что к анализу социоинженерных атак адаптируется хорошо известный формализм, который использовался для анализа атак на программно-аппаратное обеспечение (деревья атак) [5, 9, 10].

Кроме того, для уменьшения вычислительной сложности алгоритма анализа информационной системы целесообразно внести такую

информационную модель, как модель группы пользователей, позволяющую задать сразу большому числу пользователей конкретные права на доступ и использование определенных устройств. Иными словами, информационная модель групп пользователей отображает политику безопасности информационной системы по отношению к пользователям.

Среди уже упомянутых в нашей статье информационных моделей отметим модели контролируемых зон и информационных объектов. В отличие от статьи [8], мы относим к контролируемым зонам не только пользователей, но и устройства. Это также поможет в дальнейшем уменьшить вычислительную сложность алгоритма анализа информационной системы. Модель информационных объектов переносится без изменений, только информационные объекты привязываются к устройствам, и на каждом устройстве, таким образом, формируется свой набор информационных объектов.

4. Выводы. Исходя из полученных информационных моделей, можно построить полную модель информационной системы. Таким образом, получена основа для создания программного продукта, который мог бы анализировать защищенность информационной системы. Необходимость добавления всех перечисленных информационных моделей в модель информационной системы обусловлена необходимостью анализа последней именно при угрозах социоинженерных атак. В более простых случаях такое наполнение информационной системы может быть избыточным.

Алгоритм анализа социоинженерной атаки, приведенный в статье [8], применим и к более полной информационной системы, со всеми информационными моделями, указанными в этой статье, но лишь с привязкой информационных объектов к устройствам и проверкой наличия доступа к тому или иному устройству того или иного пользователя.

Подводя черту, хочется отметить, что построена вся информационная система в терминах информационных моделей, которую предстоит поместить в программный продукт, который анализирует защищенность информационной системы и учитывает угрозы социоинженерных атак.

Литература

1. *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.
2. *Котенко И. В., Степашкин М. В., Богданов В. С.* Архитектуры и модели компонен-

тов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 7–24.
3. *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.
4. *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.
5. *Сергиевский М.* Сети — что это такое // КомпьютерПресс. 1999, №10, С. 3-9.
6. *Степашкин М.В.* Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак: Дис… канд. техн. наук: СПб.: СПИИРАН, 2002. 196 с.
7. *Тулупьева Т.В., Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Степашкин М.В.* Социально-психологические факторы, влияющие на степень уязвимости пользователей информационных систем, с точки зрения социоинженерных атак // Труды СПИИРАН. 2010. Вып. 1 (12).
8. *Тулупьев А.Л., Пащенко А.Е., Азаров А.А.* Информационная модель пользователя, находящегося под угрозой социоинженерной атаки // Труды СПИИРАН. 2010. Вып. 2(12).
9. *Фролова А. Н., Тулупьева Т. В., Пащенко А. Е., Тулупьев А. Л.* Возможный подход к анализу защищенности информационных систем от социоинженерных атак // Информационная безопасность регионов России (ИБРР-2007). V Санкт-Петербургская региональная конференция. Санкт-Петербург, 23–25 октября 2007 г.: Труды конференции / СПОИСУ. СПб., 2008. С. 195–199.
10. *Фролова А. Н., Пащенко А. Е., Тулупьева Т. В., Тулупьев А. Л.* Анализ уровня защищенности информационных систем в контексте социоинженерных атак: постановка проблемы // Труды СПИИРАН. 2008. Вып. 7. СПб.: Наука, 2008. С. 170–176.
11. *Kotenko I.V., Stepashkin M.V.* Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life // Springer-Verlag Lecture Notes in Computer Science. 2005. Vol. 3685. P. 311–324.
12. *Kotenko I.V., Stepashkin M.V.* Network Security Evaluation Based on Simulation of Malefactor's Behavior // Proc. of the Intern. Conf. on Security and Cryptography (SECRYPT–2006), Setubal, 2006. P. 339–344.
13. *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.

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

Рекомендовано ТиМПИ СПИИРАН, зав. лаб. д-р физ.-мат. наук, доцент А.Л. Тулупьев.

Статья поступила в редакцию 20.11.2010.

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 автоматизации 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. **Информационные модели компонент комплекса «информационная система—персонал», находящегося под угрозой социоинженерных атак.**

В связи с тем, что одним из основных вопросов развития анализа защищенности информационных систем становится анализ угроз с учетом человеческого фактора, а анализ защищенности информационных систем по программно-технической составляющей развит достаточно хорошо, необходимо соединить эти два подхода и получить такой программный продукт, который бы выдавал полную информацию по защищенности информационной системы, в том числе и с учетом угроз социоинженерных атак. В связи с этим в данной статье рассмотрены: информационная модель пользователя, модель групп пользователей, модель контролируемых зон, модель информационных объектов, модель программно-аппаратного обеспечения и модель самой информационной системы. Совокупность этих моделей дает информационную систему, для которой можно рассчитать анализ защищенности с учетом угрозы социоинженерных атак.

В статье рассмотрены все перечисленные модели и обоснованы необходимые свойства этих моделей, которые пригодятся при анализе информационной системы. Вся информационная система разбивается на два модуля: 1) информационные модели, связанные с пользователями информационной системы; 2) программно-техническая составляющая системы. Между этими двумя модулями и внутри самих модулей присутствуют связи, по которым может распространяться атака. Вследствие того, что социоинженерная атака в текущем контексте связана с повреждением или передачей третьим лицам определенной информации изнутри информационной системы, информационные объекты решено привязать к определенным устройствам. Таким образом, каждое устройство получает определенный набор информационных объектов. Это поможет впоследствии уменьшить вычислительную сложность алгоритма анализа защищенности системы. Для этих же целей могут быть применены модели групп пользователей, а также контролируемых зон.

На данном этапе удалось полностью смоделировать информационную систему, которая может быть использована для анализа ее защищенности. Полученные результаты позволяют приступить к созданию программного продукта, предназначенного для автоматизированного анализа информационной системы с учетом угрозы социоинженерных атак.

SUMMARY

Tulupyev A.L., Paschenko A.E., Azarov A.A. **Information models of the components of complex "information system—personnel", which is under threat of socioenginering attacks.**

As one of the basic questions of development of analyzing protection of informative system becomes the analyzing of threats with the account of human factor, while the analyzing of hardware—software part of the system developed quite well, it is essential to combine this two approaches and gain a special program product, which can prepare all information about the protection of informative system, even with the threat of socioengineering attacks. Due to this facts, this paper is devoted to the informative models of user, users group, control area, informative objects, hardware — software maintenance and to the model of informative system itself. Set of these models gives informative system, for which it is possible to analyze the protection of informative system, with the threat of socioengineering attacks.

In this paper all necessary models are considered and listed, all necessary properties of this models, which will be used for analyzing, proved. Information system is divided into two parts: informative models, which are related to the user model, and hardware—software part of the system. In these parts and between them there are some links, which can be used for distribution of the attack. The information objects are adhered to the computers, because in the current context, socioengineering attack deals with damaging or larceny of the information. That's why every computer gains some set of information objects. It will probably help to improve computing complexity of algorithm of analyzing the information system. For this purposes also can be user user's group models and controlling areas.

At the given stage the model of informative system is completed, and it can be used for analyzing of the protection of informative system. Gained results allows to start the creation program product, which can be applied for analyzing information system with the risk of socioengineering attack.