E. R. Knyazeva, A. S. Zaytsev

Investigation of the Problem of IT Espionage Using Causal Diagrams

Key words: insider, espionage, system dynamics modeling and simulation

This article deals with the problem of IT espionage. Basing on the analysis of espionage incidents and existing insider models a system dynamics model of internal intruder realizing the threat of espionage has been constructed.

Е. Р. Князева, А. С. Зайцев

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ИТ-ШПИОНАЖА С ПРИМЕНЕНИЕМ ДИАГРАММ ПРИЧИННО-СЛЕДСТВЕННЫХ СВЯЗЕЙ

Исторически сложилось, что в области обеспечения информационной безопасности (ИБ) вопросу противодействия внешним угрозам уделялось гораздо больше внимания и средств. В результате на сегодняшний день современные методы и средства защиты гарантируют высокую степень защищенности от внешнего нарушителя, в то время как вопрос эффективной защиты от внутреннего нарушителя остается открытым до сих пор.

Целью работы является разработка модели внутреннего нарушителя, которая максимально поможет руководителю организации проследить формирование преступного правосознания инсайдера, спрогнозировать его дальнейшие действия и принять соответствующие решения по предотвращению инцидента информационной безопасности.

В рамках данного доклада рассматривается самая редкая внутренняя угроза ИБ — шпионаж с использованием информационной системы (ИС) организации [1]. Ввиду отсутствия среди существующих исследований определения ИТ -шпионажа сформулировано новое, основанное на определении шпионажа, приведенном в Уголовном кодексе Российской Федерации [2]. Под шпионажем (ИТ-шпионажем) в настоящей работе понимается угроза ИБ, использование внутренним нарушителем ИБ ИС организации для сбора, хищения или хранения с целью последующей передачи внешней стороне информации в целях выгоды для внешней стороны без намерения покинуть организацию после передачи информации. Если внешняя сторона является конкурирующей организацией, то применяется термин «промышленный шпионаж». В случае выступления в качестве внешней стороны иностранного государства используется термин «международный шпионаж».

Анализ современных исследований в области защиты информации от внутреннего нарушителя показывает, что в настоящий момент отсутствует полноценная и достоверная компьютерная модель, способная обнаружить и спрогнозировать поведение внутреннего нарушителя. По мнению авторов, наиболее существенные результаты в области моделирования поведения инсайдера были достигнуты научным коллективом Carnegie Mellon University Software Engineering Institute CERT Insider Threat Team (CERT). Однако поведенческая модель шпиона, представленная CERT [3], ввиду использования экспертного метода исследования и малого объема статистических данных (9 инцидентов международного шпионажа) носит описательный характер и не может быть применена для компьютерного моделирования.

В ходе настоящего исследования для построения поведенческой модели внутреннего нарушителя, реализующего угрозу шпионажа, было рассмотрено более 100 инцидентов информационной безопасности, среди которых около 20 являются инцидентами промышленного шпионажа в России и за рубежом. В рамках доклада угроза международного шпионажа не рассматривается вследствие отсутствия достаточного количества данных о преступлениях в открытом доступе. На основе [1, 3, 4] и анализа полученных из открытых источников инцидентов были выделены основные элементы системы поведения инсайдера и построена схема их взаимодействия, изображенная на рис. 1. На основании собранной статистической информации выделены характерные особенности промышленного ИТ-шпионажа, на базе которых разработана диаграмма причинно-следственных связей (ДПСС) угрозы, представленная на рис. 2.

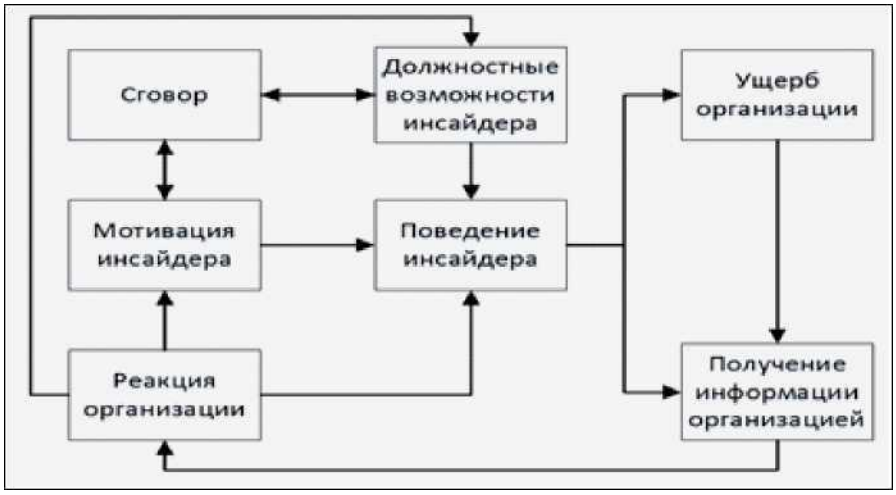

Рис. 1. Схема взаимодействия основных элементов системы поведения внутреннего нарушителя ИБ, реализующего угрозу шпионажа

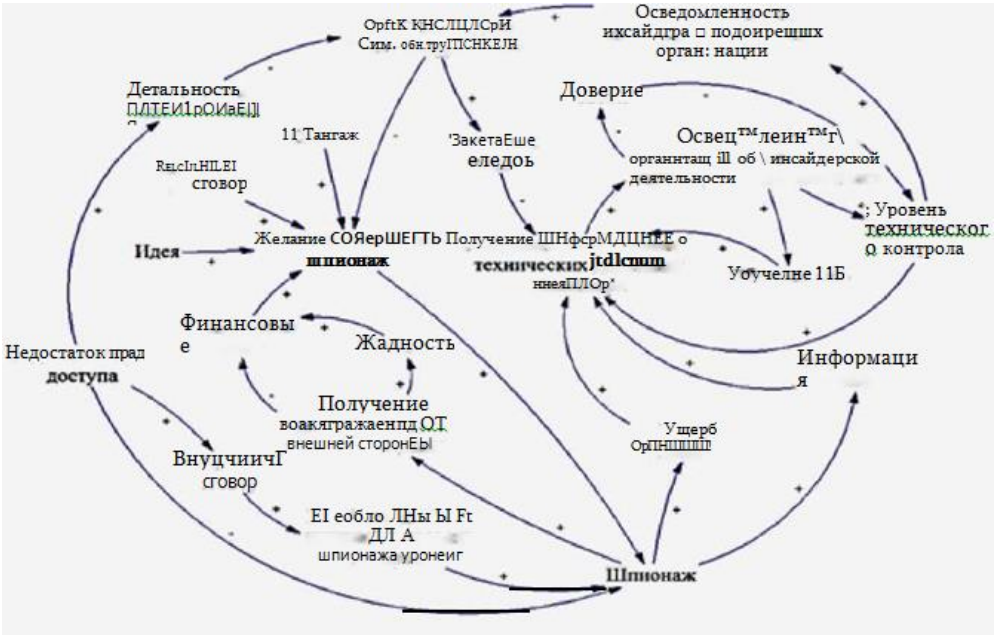

Рис. 2. Диаграмма причинно-следственных связей ИТ-шпионажа

Разработанная ДПСС помогает лучше понять поведение внутреннего нарушителя. В рамках дальнейших исследований необходимо довести полученную диаграмму до уровня прогнозной системно-динамической модели и разработать методы определения параметров модели с использованием статистической информации.

СПИСОК ЛИТЕРАТУРЫ:

1.Silowash G., Cappelli D., Moore A., Trzeciak R., Shimeall T. J., Flynn L. Common Sense Guide to Mitigating Insider Treats. 4th Edition. Software Engineering Institute. CERT Program. 2012.

2.Федеральный Закон от 13.06.1996 № 63-ФЗ «Уголовный кодекс Российской Федерации», статья 276. URL: http://www. consultant.ru/popular/ukrf/10_40.html#p5160 (дата обращения: 06.12.2014).

3.Band S. R., Cappelli D. M., Moore A. P., Shaw E. D., Trzeciak R. F. Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis. Software Engineering Institute. CERT Program. 2006.

4.Зайцев А. С., Малюк А. А. Исследование проблемы внутреннего нарушителя // Вестник РГГУ. 2012. № 14. С. 114—134.

REFERENCES:

1.Silowash G., *Cappelli D., Moore A., Trzeciak R., Shimeall T. J., Flynn L.* Common Sense Guide to Mitigating Insider Treats. 4th Edition. Software Engineering Institute. CERT Program. 2012.

2.Federal'nyi zakon ot 13.06.1996 № 63-FZ «Ugolovnyi kodeks Rossiyskoy Fedeatsii»,stat'ya 276 [Federal Law № 64-FZ of June 13, 1996 on the Enforcement of the Criminal Code of the Russian Federation, article 276]. URL: http://www.consultant.ru/ popular/ ukrf/10_40.html#p5160 (accessed 6 December 2014).

3.Band S. R., Cappelli D. M., Moore A. P., Shaw E. D., Trzeciak R. F. Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis. Software Engineering Institute. CERT Program. 2006.

4.Zaytsev A. S., Malyuk A. A. Investigation of information security internal intruder problem // RSUH/RGGU Bulletin. 2012. № 14. P. 114-134.