V. V. Ivutin, A. S. Zaytsev

Development of Behavior Model of Unintentional Insiders

Key words: unintentional insider, cause and effect diagram

The purpose of report is to increase the information security level of organization from unintentional insider threats. In the work the model and the chart of relationships of cause and effect of behavior of employees for the prevention of unintentional insider threads is presented.

В. В. Ивутин, А. С. Зайцев

РАЗРАБОТКА МОДЕЛИ ПОВЕДЕНИЯ НЕМОТИВИРОВАННОГО
ВНУТРЕННЕГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Противодействие внутреннему нарушителю является одной из наиболее актуальных и важных проблем современной информационной безопасности (ИБ), а угроза немотивированного нарушения защиты информации — одной из наименее изученных внутренних угроз ИБ [3].

Основой противодействия инсайдеру, в том числе незлоумышленному, является понимание его психологии и характера совершаемых им действий. Ввиду этого важной задачей становится разработка поведенческих моделей немотивированных внутренних нарушителей ИБ.

В современных исследованиях выделяются 4 класса немотивированных инсайдерских угроз [1, 2]:

1) утечка конфиденциальной информации;

2) порча/уничтожение важной информации;

3) потеря физического носителя;

4) манипуляция со стороны внешних нарушителей.

Нарушители, реализующие угрозы 1, 2 и 3, называются халатными, их исследованию при помощи анализа статистики инцидентов и разработки диаграммы причинно-следственных связей посвящена данная работа.

В ходе исследования было рассмотрено и проанализировано 25 инцидентов, найденных в открытых источниках. На основании полученной информации выделены основные особенности поведения халатного инсайдера и получена схема поведения халатного внутреннего нарушителя ИБ, изображенная на рис. 1.

В основе совершения сотрудником нарушения лежат человеческие факторы: его концентрация при выполнении поставленного задания и все, что на нее влияет, а также организационные факторы: уровень культуры внутри организации, осведомленность сотрудников в области ИБ. Данные факторы влияют на поведение сотрудника и в определенный момент могут привести к совершению сотрудником ошибки, приносящей ущерб организации. Компания может посредством мониторинга ИБ или наблюдения за сотрудником получить об этом информацию и принять соответствующие меры, приводящие к улучшению организационных факторов (обучение ИБ, совершенствование системы мотивации персонала, корректировка ролевой структуры и полномочий доступа, в крайнем случае — увольнение сотрудника).

Рис. 1. Схема поведения халатного немотивированного внутреннего нарушителя ИБ

На основании схемы взаимодействия основных элементов системы поведения халатного немотивированного внутреннего нарушителя ИБ разработана диаграмма причинно-следственных связей (ДПСС), изображенная на рис. 2.

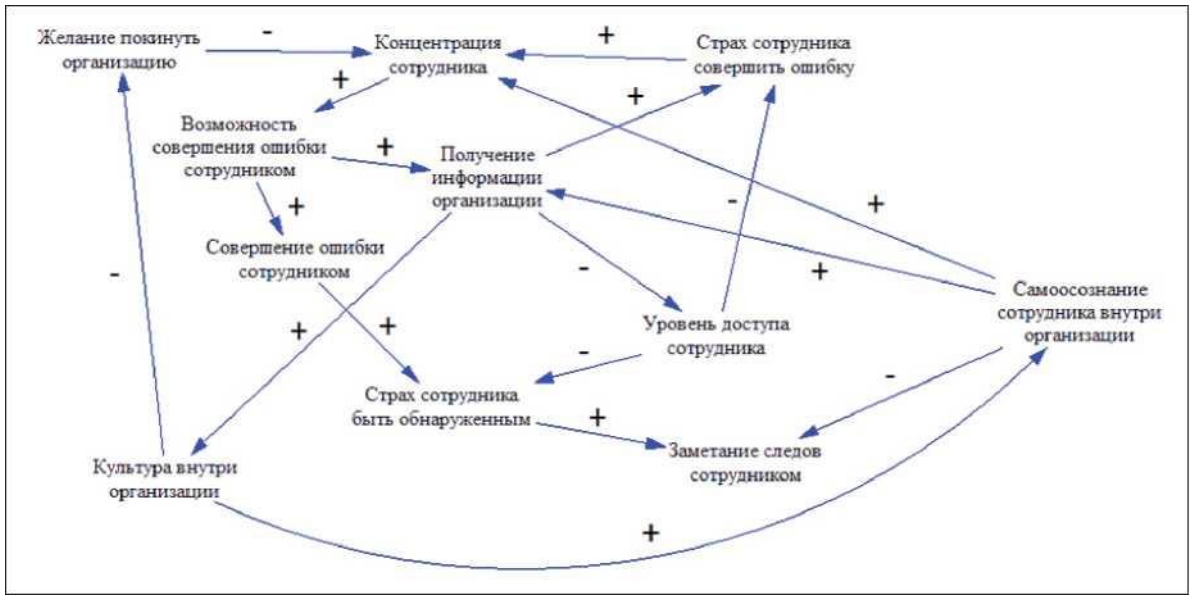

Рис. 2. Диаграмма причинно-следственных связей угрозы халатного инсайдера

Ключевым параметром ДПСС является возможность совершения ошибки сотрудником. В общем случае эта возможность зависит от множества субъективных факторов: болезней, недомогания, сонливости, чувства голода, алко- и наркозависимости, стресса [4], которые отражаются на концентрации сотрудника. Одним из не менее важных параметров ДПСС является «Самосознание сотрудника внутри организации». Параметр отражает ответственность сотрудника при выполнении поручений, умение верно оценивать пользу от своих действий для организации, чувство собственной значимости для организации.

В рамках дальнейших исследований надо расширить выборку инцидентов с участием немотивированных внутренних нарушителей ИБ, разработать ДПСС для угрозы манипулируемого инсайдера, а также полноценные прогнозные модели.

СПИСОК ЛИТЕРАТУРЫ:

1.CERT Insider Threat Team Unintentional Insider Threats: A Foundational Study —Август 2013.

2.CERT Insider Threat Center Unintentional Insider Threats: Social Engineering — Январь 2014.

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

4.Акимов В. А., Лапин В. Л., Попов В. М., Пучков В. А., Томаков В. И., Фалеев М. И. Надежность технических систем и техногенный риск. М.: ЗАО ФИД «Деловой экспресс», 2002. — 368 с.

REFERENCES:

1.CERT Insider Threat Team Unintentional Insider Threats: A Foundational Study —August 2013.

2.CERT Insider Threat Center Unintentional Insider Threats: Social Engineering — January 2014.

3.Zaytsev A. S., Malyuk A. A. Issledovanie problemy vnutrennego narushitelya // Vestnik RGGU. 2012. № 14. P. 114 — 134 p.

4.Akimov V. A., Lapin V. L., Popov V. M., Puchkov V. A., Tomakov V. I., Faleev M. I. Nadezhnost’ tehnicheskih sistem i tehnogennyi risk. M.: ZAO FID “Delovoj ekspress”, 2002. — 368 p.