M. A. Kalyakin, A. S. Zaytsev

Research of IT-fraud Threat Using Causal Relationship Diagrams

Key words: insider, information security, fraud

The study deals with the problem of building causal relationship diagram of insider conduct involving fraud.

М. А. Калякин, А. С. Зайцев

ИССЛЕДОВАНИЕ УГРОЗЫ ИТ-МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ДИАГРАММ ПРИЧИННО-СЛЕДСТВЕННЫХ СВЯЗЕЙ

В исследованиях в области обеспечения информационной безопасности основное внимание уделено нарушителю извне и довольно редко рассматривается появление внутреннего нарушителя, что связано со сложностью этой проблемы, которая должна учитывать психологические и поведенческие аспекты, с трудом поддающиеся оценке и анализу.

Управление «К» МВД России утверждает, что самыми массовыми киберпреступлениями являются действия обычных мошенников, которые «осваивают» Интернет. Специалисты Управления отмечают, что порядка 80 % заявлений граждан содержат сведения именно о таких преступлениях [4]. Исходя из данных МВД мошенничество является доминирующим способом преступной активности в ИТ-сфере.

Задача данного исследования — разработка модели поведения внутреннего нарушителя ИБ, реализующего угрозу мошенничества с использованием информационных систем организации (ИТ -мошенничество). Данной теме посвящен ряд опубликованных работ, в частности [2], в которой произведен анализ психологии и поведения ИТ -мошенника, а угроза ИТ -мошенничества подразделяется на две различные категории: ИТ -мошенничество на руководящей должности и ИТ-мошенничество на неруководящей должности, и [3], в котором исследовано мошенничество в целом и выделены технические и поведенческие индикаторы мошенника.

В рамках нашего исследования был проведен поиск в открытых источниках информации преступлений, совершенных внутренними нарушителями ИБ. В результате была составлена база инцидентов, в которую входит более 100 различных преступлений. Среди них было выделено 20 случаев ИТ -мошенничества. В результате анализа собранной информации были выявлены основные особенности данного типа внутреннего нарушителя и потенциально реализуемые им угрозы. Существенных различий для мошенничества на руководящей и неруководящей должностях не обнаружено на исследованной статистической выборке.

На основании исследованных инцидентов разработана схема взаимодействия основных элементов системы поведения ИТ -мошенника, изображенная на рис. 1.

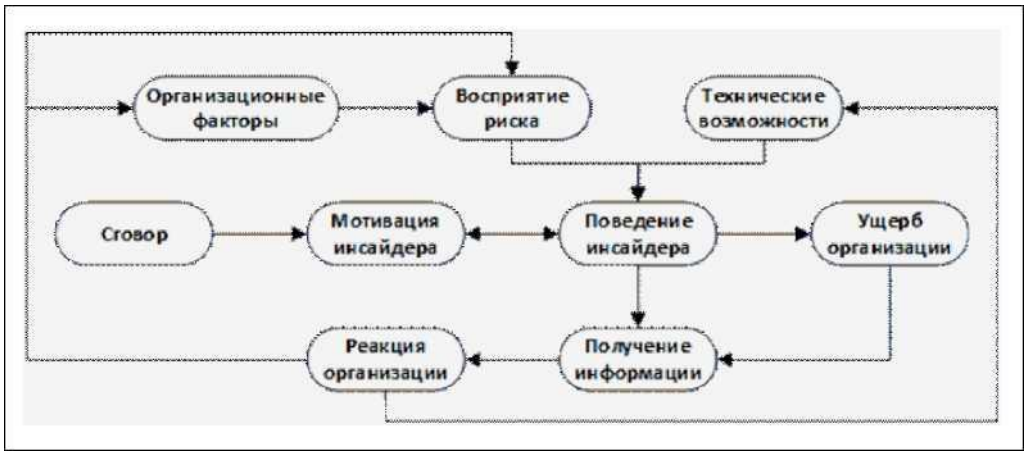

Рис. 1. Схема взаимодействия основных элементов системы поведения ИТ-мошенника

При детализации взаимодействующих элементов с учетом особенностей поведения, выявленных на этапе сбора и анализа инцидентов, была построена диаграмма причинноследственных связей, изображенная на рис. 2.

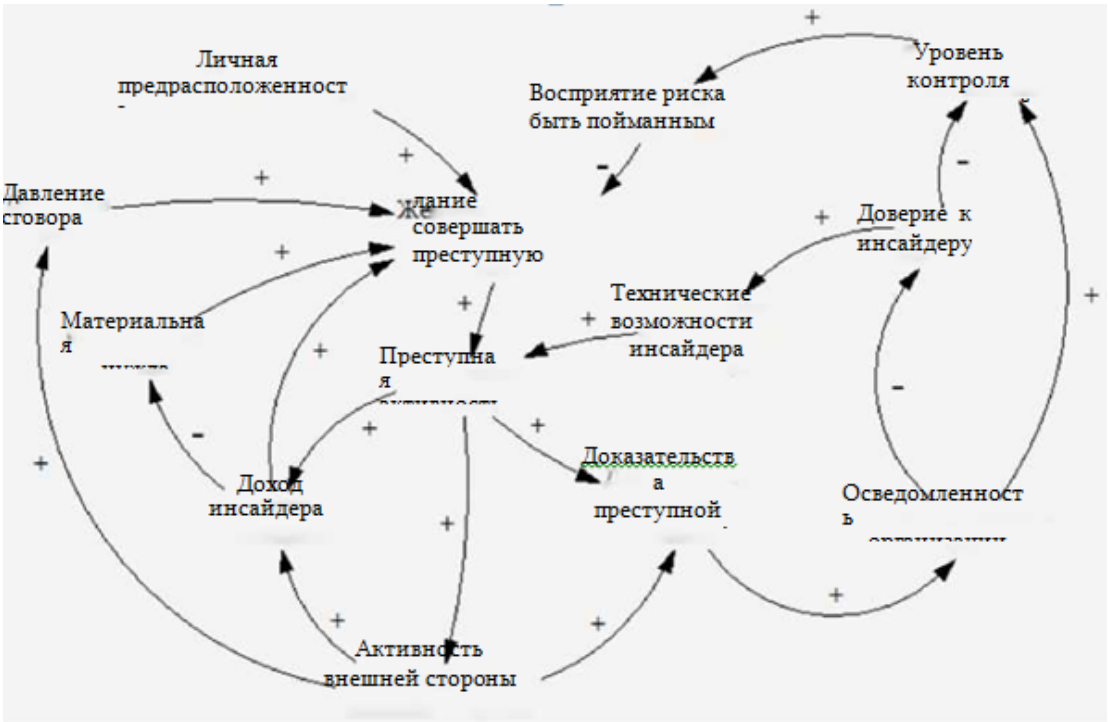

Рис. 2. Диаграмма причинно-следственных связей ИТ-мошенничества

В рамках дальнейших исследований необходимо преобразовать полученную диаграмму причинно-следственных связей в диаграмму потоков (системно-динамическую модель) и произвести с ее помощью прогнозное моделирование. Также необходимо исследовать возможность обучения моделей с использованием собранной статистической информации.

СПИСОК ЛИТЕРАТУРЫ:

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

2.Cummings A., Lewellen T., McIntire D., Moore A. P., Trzeciak R. Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector. Software Engineering Institute. CERT Program. 2012.

3.FRAUD INDICATORS - The Office of the Inspector General for USAID. 2013.

4.Вураско А. По IT-криминалу — «ликбезом» // BIS Journal — Информационная безопасность банков. 2014. № 2 (13). С. 10-15.

REFERENCES:

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

2.Cummings A., Lewellen T., McIntire D., Moore A. P., Trzeciak R. Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector. Software Engineering Institute. CERT Program. 2012.

3.FRAUD INDICATORS — The Office of the Inspector General for USAID. 2013.

4.Vurasko A. Po IT-kriminalu — «likbezom» // BIS Journal — Informatsionnaya bezopasnost bankov. 2014. № 2 (13). P. 10—15.