

favor, often destroying or misusing the personal information of other people that are using those specific services. To prevent future risks, e-commerce service providers should acknowledge that there is no completely secure system and that their web site should be

permanently tested for vulnerabilities that may compromise end-users. Also, the software providers for e-commerce services should promote good coding practices, so less vulnerabilities are available in the core of the system, rather than on the end-user machine.

Bibliography:

1. <http://www.securityfocus.com/infocus/1775>
2. <http://msdn.microsoft.com/en-us/magazine/cc163917.aspx>
3. <http://msdn.microsoft.com/en-us/library/ms998274.aspx>

Иван Сорбат,

Харьковский национальный экономический университет (Украина)

МЕТОД СОЦИОМЕТРИИ В ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

The purpose of given article is formalizing of the task of revealing insider at firm (organization) a method sociometry. The revealing task insider at firm (organization) is actual. For its solution basically heuristic methods which, as is known, have big enough error are used. Besides, solution of the task of revealing insider in mathematical setting is difficultly formalized.

На сегодняшний день умышленная или неумышленная деятельность инсайдеров в большинстве случаев приводит к убыткам и потерям в прибыли, снижению экономического роста предприятия, страны в целом, что подтверждают исследования в этой области.

Как известно, инсайдер – пользователь информационной системы, имеющий вполне легальный доступ к информации с ограниченным доступом (конфиденциальная, коммерческая, банковская, персональная и т.д.) и применяющий весь арсенал

доступных ему средств для того, чтобы использовать эту информацию в своих интересах [1].

Следовательно, возникает актуальная задача выявления инсайдеров на предприятии (организации). Для ее решения в основном используются эвристические методы, которые, как известно, имеют довольно большую погрешность и не дают требуемого результата. Кроме того, решение задачи выявления инсайдеров в математической постановке является трудно формализуемым, и требует проведение множества практических экспериментов.

Целью данной статьи является формализация задачи выявления инсайдеров на предприятии (организации) методом социометрии.

Предлагаются результаты исследований компаниями Compuware и Ponemon Institute в области экономической безопасности [2]. Исследования проводились с помощью запатентованных онлайн-овых платформ, в котором приняло участие 3596 IT-специалистов. Как оказалось, из-за действий хакеров на предприятиях осуществляется лишь 1% утечек, в то время как 75% случаев происходит в результате неосторожных действий невнимательных сотрудников, (например, потеря ноутбука или устройств флэш-памяти). При этом 24% инсайдеров разглашают секретную информацию намеренно – с корыстными или иными целями.

Исследованием этой проблемы в методологических аспектах занимались следующие авторы: Геєць В. М., Ярочкин В. И., Домарев В. В., Олейников Е. А., Кавун С. В., Кизим М. О. [3-8]. В данных работах были исследованы вопросы систематического подхода для устранения угроз информационной и экономической безопасности, но в большей части эти исследования касаются внешних угроз. Не до конца решенным остается вопрос внутренних угроз, а именно вопрос выявления инсайдеров.

Для решения задачи выявления предполагаемого инсайдера, предлагается воспользоваться одним из методов социометрии.

Термин «социометрия» образован от двух латинских корней: socius

– товарищ, компаньон, соучастник и tetrum – измерение. Основная заслуга в создании определенной методологии социометрических исследований, совокупности измерительных процедур и математических методов обработки первичной информации принадлежит американскому социопсихологу Джекобу Морено. Исходя из практики исследований, оптимальным принято считать численный состав малого коллектива в 10-20 человек. В некоторых случаях этот предел увеличивается до 40 человек. При таких условиях методы социометрии еще применимы.

При социометрическом опросе каждому опрашиваемому вручается социометрическая анкета (социометрическая карточка) и список членов социометрируемой группы. Для удобства работы и последующей обработки фамилии членов группы шифруются, в простейшем случае – кодируются номером в списке группы. Карточка оформляется в следующем виде (табл. 1).

Результаты опроса заносятся в социоматрицу, представляющую первичную информацию и упрощающую последующую математическую обработку собранных данных.

Матрица представляет собой таблицу, в которую по строкам помещают ответы каждого из членов группы. В таблице 2 приведены итоги непараметрического социометрического опроса шести членов группы по дихотомическому критерию: «+» – означает предпочтение (положительный выбор), «-» – отвержение (отрицательный выбор), «0» – фиксирует отсутствие выбора.

Таблица 1

Социометрическая карточка для непараметрической процедуры

Критерии	Укажите номера членов начальства из списка
1. Кого бы Вы хотели видеть в качестве своего начальника?	
2. Кого бы Вы не хотели видеть в качестве своего начальника?	
3. Кто может предложить Вас в качестве начальника?	
4. Кто не предложит Вас в качестве начальника?	

Таблица 2

Социоматрица

Кто выбирает		Кого выбирают						Число выборов		
		1	2	3	4	5	6	+	-	всего
1	Евсеев	+	-	+	+	-	-	2	3	5
2	Бондарев	0	+	0	+	0	+	2	0	2
3	Михайлов	+	-	+	+	0	0	2	1	3
4	Самойленко	0	0	+	+	0	+	2	0	2
5	Поляков	0	-	0	+	+	0	1	1	2
6	Чинов	+	+	+	+	0	+	4	0	4
Число полученных выборов:		+	2	1	3	5	0	2	13	
		-	0	3	0	0	1	1		5
Всего:			2	4	3	5	1	3		18

Самовыбор не предполагался, поэтому по диагонали ставим знак «+». Уже визуальный анализ социоматрицы многое говорит о взаимоотношениях в группе: как члены группы выбирают и кого, кто более активно выбирается, кто чаще отвергается. Удобным способом представления содержания социоматрицы являются сопрограммы, которых имеется множество видов. Укажем только одну из простейших – круговую социограмму. В этом случае все члены

группы располагаются симметрично на окружности, и соответствующие линии отражают межличностные связи между членами группы.

Таким образом, формализуемая задача выявления инсайдеров сводится к задаче оптимизации и применения метода социометрии в экономической безопасности. В дальнейшем данное исследование можно совершенствовать и использовать по предложенной методике.

Литература:

1. Кавун С. В. *Информационная безопасность в бизнесе*: Монография. – Х.: ХНЕУ, 2007. – 408 с.
2. Compuware Study Shows Insiders Pose Biggest Threat to Data Security // http://www.compuware.com/pressroom/news/2007/7185_ENG_HTML.htm.
3. Кавун С. В. *Жизненный цикл системы экономической безопасности предприятия* // Управління розвитком. – 2008. – № 6. – С.17-21.
4. Кавун С.В., Сорбат И.В. *Инсайдер – угроза экономической безопасности* // Управління розвитком. – 2008. – № 6. – С.7-11.
5. Домарев В. В. *Безопасность информационных технологий. Методология создания систем защиты*. – К.: ООО «ТИД «ДС», 2001. – 688 с.
6. Дорошев В. В. *Рекомендации по обеспечению безопасности конфиденциальной информации согласно «Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)», США, «Оранжевая книга»* / В. В. Дорошев, В. В. Домарев // Бизнес и безопасность. – 1998. – № 1. – С.19-21.
7. Олейников Е. А. *Экономическая и национальная безопасность: Учебник для вузов*. – М.: Экзамен, 2005. – 768 с.
8. Геєць В. М. *Моделювання економічної безпеки: держава, регіон, підприємство*: Монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк. – Х.: ХНЕУ, 2006. – 240 с.

Svetlana Ghetmancenco, ASEM

PROBLEMATICA IMPLEMENTĂRII SISTEMULUI DE MANAGEMENT AL CALITĂȚII ÎN TEHNOLOGIILE INFORMAȚIONALE

Like an extension of my last material about implementation of the quality of management information systems, this article is about the quality of management activities and management of business partnerships. Also, we must see how the procedures are changed for IT starting from ISO9001 standard.

Keywords: *quality management, standard, information and communication technology, partnership.*

În condițiile trecerii la societatea informațională, proces complex care implică adoptarea de instrumentare informatice performante, menite să asigure

accesul rapid la informații și valorificarea adecvată a acestora în procesul decizional, tehnologiile informaționale capătă o importanță deosebită.