необходимых мер защиты (организационных, финансовых, юридических); внедрение дополнительно принятых мер защиты с учетом установленных приоритетов, доведение до персонала организации реализуемых мер, осуществление контроля; мониторинг и корректировка внедренных мер целью анализа работоспособности созданной системы безопасности информации.

МЕТОД ВЫЯВЛЕНИЯ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ

С. КАВУН, И. СОРБАТ,
Харьковский национальный экономический университет (Украина)

Актуальность. Предприятия и организации, банковские и финансовые учреждения, IT-компании разных стран Европы, США, России и Украины несут огромные финансовые потери вследствие экономической преступности и халатности сотрудников организаций, так называемой инсайдерской деятельности. Следовательно, возникает необходимость решения актуальной задачи выявления инсайдера или группы инсайдеров (инсайдерской деятельности), ответственных за утечку определенных категорий конфиденциальных данных в организации (на предприятии).

Над проблемами в данной сфере работают многие известные специалисты и ученые: Верин В.П., Гуров М.П., Олейников Е. А., Кизим М.О., Куркин Н.В., Шкарлет С.Н., Кавун С.В. и др. [1-8] В их 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, и, как следствие, вопрос выявления (обнаружения) инсайдеров.

Целью статьи является представление нового метода, который позволит решить задачу выявления инсайдеров (инсайдерской деятельности) в организации (на предприятии).

Основной материал. По результатам анализа отчетов аналитических компаний – предлагается разделить предприятия и организации, в которых произошли обнародованные утечки на три категории: государственные учреждения, коммерческие предприятия, а так же учебные заведения и общественные не коммерческие структуры, для которых рассчитаны распределения источников утечек по видам организаций (табл. 1).

Для определения наиболее важных данных, подвергшихся утечке, выделено три основные категории конфиденциальной информации: персональные данные, государственная и коммерческая тайны. Подавляющее число инцидентов (90-98%) за весь период наблюдений охватывают персональные данные, что затрудняет выделение тенденций. Также получены распределения утечек по типам конфиденциальных данных (табл. 2).

Таблица 1

Распределения источников утечек по видам организаций

№	Вид организаций	1 полугодие 2009		1 полугодие 2010	
		Кол-во	%	Кол-во	%
1	Коммерческие	265	64,2	296	73,8
2	Государственные	88	21,3	61	16,0
3	Образовательные и не коммерческие	43	10,4	127	8,1
4	Не установлено	17	4,1	8	2,1

Таблица 2

Распределения утечек по типам конфиденциальных данных

№	Тип конфиденциальных данных	1 полугодие 2009		1 полугодие 2010	
		Кол-во	%	Кол-во	%
1	Персональные данные	360	87,2	374	97,9
2	Коммерческая тайна, ноу-хау	12	2,9	2	0,5
3	Государственная и военная тайна	9	2,2	2	0,5
4	Другая конфиденциальная информация	28	6,8	4	1,0
5	Не установлено	4	1,0	0	0

Полученные результаты анализа позволяют предложить новый метод выявления инсайдерской деятельности, который основывается на использовании некоторой совокупности критериев (признаков) – $\{p_i\}$, по которым можно выявить инсайдеров причастных к утечке данных в организациях. Для этого необходимо построить матрицу критериев (признаков) $P = \{p_i\}$.

Выводы. Общее число утечек продолжает оставаться на уровне примерно 2 инцидента / сутки. При этом имеются основания полагать, что количество скрытых утечек столь же велико, как и количество обнародованных, а, возможно, и существенно превосходит их. В государственных и негосударственных, коммерческих и некоммерческих организациях должны использоваться одинаковые методы выявления мошенничества и защиты от утечек данных.

Для дальнейшего исследования предлагается построить новый критериальный метод выявления инсайдеров применив разработанный авторами статьи специальный подход системы фильтрации, а так же его формализация в математическом виде.

Литература:

1. Верин В.П., Преступления в сфере экономики. - М., Дело.2002.
2. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия // Управління розвитком. – 2008. – № 6. – С.17-21.
3. Кавун С.В., Сорбат И.В. Инсайдер – угроза экономической безопасности // Управління розвитком. – 2008. – № 6. – С.7-11.
4. Кавун С.В. Математическая интерпретация задачи выявления инсайдеров в организации (предприятии)// Кавун С.В., Сорбат И.В. – Научный журнал "Эконо-

мика: проблемы теории и практики". Днепропетровск: Изд. Руснаука, 2009. – т. 246. – № 4. – С. 862-869.
5. Олейников Е. А. Экономическая и национальная безопасность: Учебникдля вузов. – М.: Экзамен, 2005. – 768 с.
6. 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.
7. Гуров М.П., Кудрявцев Ю.А. Теневая экономика и экономическая преступность в вопросах и ответах: Учебное пособие. - СПб.: Санкт-Петербургский университет МВД России, 2002. - 237 с.

ФОРМИРОВАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТОРГОВОЙ КОМПАНИИ

С. В. КАРПЕНКО, Е.В. ПРОКОФЬЕВА
Белорусский торгово-экономический университет потребительской кооперации (Гомель, Республика Беларусь)

В сфере информационных технологий растет объем предложений по обеспечению безопасности информационных систем. Действия служб, направленные на повышение уровня информационной безопасности, не приносят доходов, но с их помощью можно уменьшить потери от возможных инцидентов.

Потребности организации в некотором уровне защищенности автоматизированной системы можно определить, воспользовавшись руководящими стандартами СТБ 34.101.1 - 2001(ИСО/МЭК 15408-1-99), ("Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий").

Требования к автоматизированным системам защиты обобщены в таблице 1, где выполнен анализ системы защиты информации, условно состоящей из следующих четырех подсистем: подсистема управления доступом; подсистема регистрации и учета; криптографическая подсистема; подсистема обеспечения целостности.

Таблица 1

Требования к автоматизированным системам защиты

Подсистемы и требования	Класс 3	Класс 2	Класс 1

Анализ данных таблицы и сопоставление ее характеристик с реальными характеристиками технологий и программных продуктов предприятия позволяет говорить о принадлежности корпоративной информационной системы компании к 1 классу и отметить достаточно высокий уровень соответствия.