5. *Марченко Б.Г.* Линейные случайные процессы и их приложения / *Б.Г. Марченко, Л.Н. Щербак*. – К.: Наукова думка, 1975. – 144 с.
6. *Марченко Б.Г.* Вибродиагностика подшипниковых узлов электрических машин / *Б.Г. Марченко, М.В. Мыслович*. – К.: Наукова думка, 1992. – 196 с.
7. *Марченко Б.Г.* Лінійні періодичні процеси / *Б.Г. Марченко* // Праці Ін-ту електродинаміки НАНУ. – К.: ІЕД НАНУ, 1999. – с.172-185; 1999. – с. 172-185.
8. *Мыслович М.В.* Периодически коррелированные случайные процессы в задачах обработки акустической информации / *М.В. Мыслович, Н.В. Приймак, Л.Н. Щербак*. – К.: Об-во ''Знание'' УССР,1980. – 28 с.
9. *Рытов С.М.* Введение в статистическую радиофизику. Ч.2. Случайные поля / *С.М. Рытов, Ю.А. Кравцов, В.И. Татарский*. – М.: Наука, 1978. – 420 с.
10. *Самарский А.А.* Современная прикладная математика и вычислительный эксперимент / *А.А. Самарский* // Коммунист. – 1983. – № 8. – С. 31-42.

Поступила 31.01.2011р.

УДК 519.8

А.М. Богданов, д.т.н., ИССЗИ НТУУ «КПИ», г. Киев
В.В. Мохор, д.т.н., ИССЗИ НТУУ «КПИ», г. Киев

О МОДЕЛИРОВАНИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ ПРОЦЕССНОГО ПОДХОДА

Предлагается использование процессного подхода при разработке моделей систем управления информационной безопасностью.

Пропонується використання процессного підходу при розробці моделей систем управління інформаційною безпекою.

Designing of the models information security management systems are proposed to perform on the base of process approach.

Ключові слова: моделювання, системи управління інформаційною безпекою, процессний підхід.

При анализе международного стандарта построения систем управления информационной безопасностью (СУИБ) ISO 27001:2005 [1] как «лучшей на сегодняшний день мировой практики построения СУИБ» обращает на себя внимание подход, который положен в его основу. Как, впрочем, и в основу некоторых других популярных в настоящее время международных стандартов управления качеством в различных сферах. Например, стандарта ISO 9001:2008 [2] управления качеством производимых товаров и услуг.

Подход этот называется «процессным подходом» и представляет собой «преобразование входных величин в выходные величины с использованием определенных ресурсов и под воздействием определенного управления». То есть рассматривается воздействие ВО ВРЕМЕНИ некоторого возмущения на объект, обладающий определенными ресурсами и управляющийся (или самоуправляющийся) по определенному алгоритму. На выходе объекта получается реакция его на поступившее возмущение.

Такой подход приводит к мысли об аналогии процессов управления информационной безопасностью и процессов, протекающих в электрических цепях, а также их анализе и оптимизации с помощью известных математических методов (операторный, символический, частотный и др. [3]).

В этом плане информационная безопасность может рассматриваться как «устойчивое течение процесса управления объектом (или самоуправления объекта) в пределах допустимых отклонений от идеального предписанного режима в условиях целенаправленных сторонних или внутренних попыток вывести управляемый объект из предписанного режима [4]».

Из этого определения явно просматриваются такие хорошо известные из курсов Теории электрических цепей понятия, как «передаточная функция объекта», «характеристическое уравнение и характеристический полином», «критерии устойчивости работы (Гурвица, Найквиста и др.)», «допустимые отклонения параметров объекта» и т.п. Проясняется и назначение системы информационной безопасности – иметь такую передаточную функцию, которая бы в комплексе с передаточной функцией объекта обеспечила его устойчивую работу при заданных ограничениях на величину возмущений. Как внешних, так и внутренних. Как случайных, так и преднамеренных.

Для реализации изложенной идеи прежде всего необходимо разобраться, а что же все-таки является процессом при рассмотрении информационной безопасности? Если при производстве товаров и услуг (сфера стандарта ISO 9001:2008) это – процесс в основном производственный, когда с использованием ресурсов производится продукт с заданными качественными характеристиками, то в информационной безопасности (стандарт ISO 27001:2005) – это будет процесс нанесения ущерба предприятию вследствие нарушения определенного его информационного актива. Нарушению могут подвергаться такие характеристики информационного актива как конфиденциальность, целостность или доступность информации, заключенной в активе. Ущербом являются реальные и потенциальные потери предприятия в настоящем или в будущем времени.

Естественно, система управления информационной безопасностью для данного актива должна быть синтезирована таким образом, чтобы весь комплекс (информационный актив, его уязвимости, возможные угрозы нарушения актива, система защиты информации) минимизировал в итоге ущерб, возникающий от данной угрозы. А в идеале – от всех угроз сразу.

В крупном плане алгоритм реализации данного подхода к моделированию СУИБ можно представить следующими этапами:

1. Детально рассматривается (во времени) механизм воздействия на информационный актив:

а) угроз из 1-ой группы угроз по классификации IT-Grundschutz [5] – форс-мажорных обстоятельств (наводнения, землетрясения, общественные беспорядки и т.п.);

б) угроз из 2-ой группы (несовершенство организации работы предприятия);

в) угроз из 3-ей группы (из-за человеческого фактора);

г) угроз из 4-й группы (технические отказы);

д) угроз из 5-й группы (преднамеренные умышленные действия).

2. Проводится формальное математическое описание рассмотренных процессов воздействия угроз как в частных, так и в общем случае.

3. Определяются механизмы противодействия влиянию рассмотренных угроз.

4. Синтезируется СУИБ по критерию обеспечения минимального ущерба от нарушения информационных активов предприятия.

При этом в процессе работы задаются допустимые пределы изменения параметров составных частей модели, исследуется робастность полученных алгоритмов.

Таким образом, общим итогом применения процессного подхода к исследованию СУИБ должны явиться рекомендации по построению СУИБ и выбору их параметров на основе строгих и адекватных математических моделей.

1. ISO/IEC 27001:2005 “Information technology – Security techniques – Information security management systems - Requirements”.

2. ISO 9001:2008 “Quality management systems — Requirements”.

3. *Белецкий А.Ф.* Основы теории линейных электрических цепей. – М.: Связь, 1967. – 608 с.

4. Достаточно общая теория управления (редакция 2004 года). Постановочные материалы учебного курса факультета прикладной математики — процессов управления Санкт-Петербургского государственного университета (1997-2003 гг.). – www.kob.org.ua.

5. IT-Grundschutz-Kataloge. — https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/it-grundschutz-kataloge_2005_pdf_en_zip.zip?__ blob= publication File

Поступила 14.02.2011р.