1. *Соловьев В., Дембицкий Ю.* Не вооружен, но очень полезен: применение беспилотных авиационных комплексов в народном хозяйстве // Авиапанорама. – №6. – К.: 2008. – С.28-32.
2. *Ильченко М.Е., Кравчук С.А.* Телекоммуникационные системы на основе высотных аэроплатформ. – К.: Наукова думка. 2008. – 580с.
3. *Лисенко О.І., Валуйський С.В.* Метод оптимального управління топологією мережі безпілотних літальних апаратів за критерієм підвищення зв'язності безпроводових ad-hoc мереж // Збірник наукових праць «Системи управління, навігації та зв'язку». – Вип.2(14). – К.: 2010. – С.218-224.
4. *Han Z., Swindlehurst A.L., Liu K.J.R.* Smart deployment/movement of unmanned air vehicle to improve connectivity in MANET // in Proc. IEEE Wireless Commun. Netw. Conf. 2006. – pp.252-257.
5. *Миночкин А.И., Романюк В.А.* Управление качеством обслуживания в мобильных радиосетях // Зв'язок. – №8. – К.: 2005. – С.17-24.
6. *Прокис Дж.* Цифровая связь. Пер. с англ. / Под ред. Д.Д. Кловского. – М.: Радио и связь. 2000. – 800с.
7. *Conan J.* The weight spectra of some short low rate convolutional codes // IEEE Trans. on Comm. – vol.32, №9. – 1984. – pp.1050-1053.
8. *Давыдов А.В., Ломаев А.А.* Улучшенная оценка вероятности пакетной ошибки сверточных кодов в релеевском канале с независимыми замираниями // Труды Научной конференции по радиофизике (Нижний Новгород, 7 мая, 2005г.). – Т.1. – Нижний Новгород: 2005. – С.194-195.

Поступила 20.10.2010р.

УДК 004.056

А.М. Богданов, д-р техн. наук, ИССЗИ НТУУ «КПИ», г. Киев,
В.В. Мохор, д-р техн. наук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев

РАЗРАБОТКА МОДЕЛЕЙ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ ПОЛНОЙ ФУНКЦИИ УПРАВЛЕНИЯ

Вопросы минимизации ущерба предприятий и организаций из-за нарушения их информационных активов с каждым днем приобретают все большую актуальность. С одной стороны, бурное развитие информационных технологий открывает все большие возможности для реализации самых, казалось бы, фантастических замыслов по доступу к информации конкурентов, ее хищению, умышленному изменению, блокированию.

С другой стороны, процессы информационных воздействий плохо поддаются формализации, математическому анализу и оптимизации в силу того, что они являются нестационарными случайными процессами с множеством неизвестных параметров. Основную нестационарность «обеспечивает» злоумышленник, вносящий изменения в процесс

функционирования информационного актива случайным (по крайней мере, для нас) образом, то есть когда захочет и как захочет. Другими словами, в этих задачах нам противостоит интеллект человека, то есть его способность генерировать новые для него информационные модули по мере возникновения потребности в них.

И с третьей стороны, сам предмет воздействия и защиты, – информация – в принципе отличается от материальных объектов и не позволяет из-за этого использовать при ее изучении уже известные результаты, например, из производственной деятельности людей. В частности, если материальные объекты подчиняются законам сохранения массы и энергии, то к информации они не применимы. То есть, если из ведра через некоторое отверстие вытекает вода, и воды в ведре становится все меньше и меньше, то при утечке информации из головы системного администратора фирмы к конкурентам эта информация полностью сохраняется там, откуда утекает. Поэтому в случае с водой утечка обнаруживается достаточно просто, а в случае с информацией – нет.

Из-за перечисленных особенностей информационной безопасности (ИБ) как предмета исследований до сих пор не найдено общепринятых теоретических решений по построению оптимальных систем ИБ. Поэтому любые усилия в данной области являются желательными, злободневными и полезными.

На сегодняшний день уже имеются результаты по построению систем управления информационной безопасностью (СУИБ) в практической области, на уровне организационных рекомендаций по постановке данного вида деятельности на предприятии. Речь идет о линейке международных стандартов серии ISO 27000, основным из которых является стандарт ISO 27001:2005 «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования» [1]. Этот стандарт считается лучшей мировой практикой по построению СУИБ на данный момент.

Мы посмотрим на управление информационной безопасностью с позиций так называемой полной функции управления (ПФУ). Это понятие введено и достаточно подробно исследовано в курсе достаточно общей теории управления [2]. Но практические примеры там берутся в основном из социальной сферы деятельности.

Итак, что же такое ПФУ? Полная функция управления – это совокупность разнокачественных действий, которая включает в себя следующие этапы:

1. Выявление фактора среды, который «давит на психику», чем и вызывает *субъективную* потребность в управлении. *Управление по полной функции начинается именно с этого.*
2. Формирование навыка (стереотипа) распознавания фактора среды на будущее и распространение его в базе знаний общества.
3. Целеполагание в отношении выявленного фактора.

По своему существу целеполагание представляет собой формирование вектора целей управления в отношении данного фактора и внесение этого вектора целей в общий вектор целей субъекта-управленца. Целеполагание может включать в себя решение задачи об устойчивости частных целей и вектора целей в целом в смысле предсказуемости поведения объекта, хотя это может быть отнесено и к этапу 4 полной функции управления.

4. Формирование генеральной концепции управления и частных концепций управления в отношении каждой из целей в составе вектора целей (т.е. целевых функций управления, составляющих в совокупности генеральную концепцию) на основе *решения задачи об устойчивости в смысле предсказуемости поведения объекта (процесса) под воздействием: внешней среды, собственных изменений объекта, управления им*.

5. Внедрение генеральной концепции управления в жизнь – организация новых или реорганизация существующих управляющих структур, несущих целевые функции управления.

6. Контроль (наблюдение) за деятельностью структур в процессе управления, осуществляемого ими, и координация взаимодействия разных структур.

7. Ликвидация существующих структур в случае ненадобности либо поддержание их в работоспособном состоянии до следующего использования.

Полная функция управления может осуществляться только в интеллектуальной схеме управления, которая представляет собой разновидность схемы управления «предиктор-корректор». В свою очередь схема управления «предиктор-корректор» может быть представлена как сочетание предсказателя (предиктора) и программно-адаптивного модуля (корректора). Работе предиктора соответствуют 1-4 этапы ПФУ, а работе программно-адаптивного модуля соответствуют этапы ПФУ 5-7 (хотя реально предиктор контролирует и эти этапы в ходе своей деятельности, а также отчасти соучаствует в их реализации).

Таким образом, для качественного управления информационной безопасностью предприятия необходимо, прежде всего, уметь предсказывать поведение системы ИБ как объекта управления в различных жизненных условиях. То есть предсказание должно быть многовариантным с возможностью выбора конкретного варианта для конкретных условий функционирования. Эту задачу выполняет интеллектуальная часть схемы управления – предиктор-предсказатель. Он реализует этапы 1-4 ПФУ. Далее СУИБ запускается в работу. Работа проходит в адаптивном режиме с периодическим контролем качества функционирования и подстройки параметров СУИБ. Это – этапы 5 и 6 ПФУ. Заканчивается все ликвидацией СУИБ тогда, когда она будет уже не нужна, или же консервацией ее элементов в случае, когда предполагается ее использование в будущем. Это – последний, 7-й этап ПФУ. Этапы 5-7 реализуются программно-адаптивным модулем СУИБ.

Обратимся теперь еще раз к стандарту ISO 27001:2005. Он основан на модели «Plan-Do-Check-Act» (PDCA) структуризации всех процессов, протекающих в СУИБ (Рис.1).

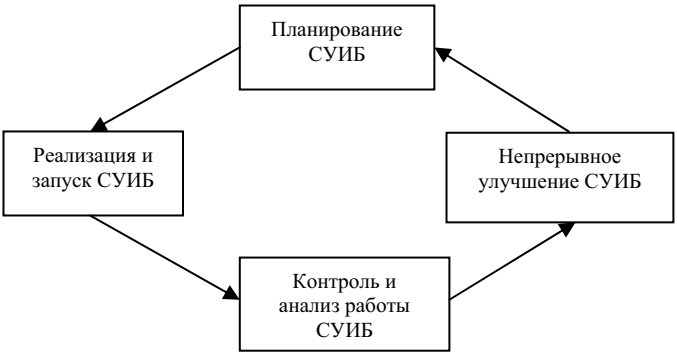

Рис. 1. Модель PDCA, примененная в [1] к процессам СУИБ

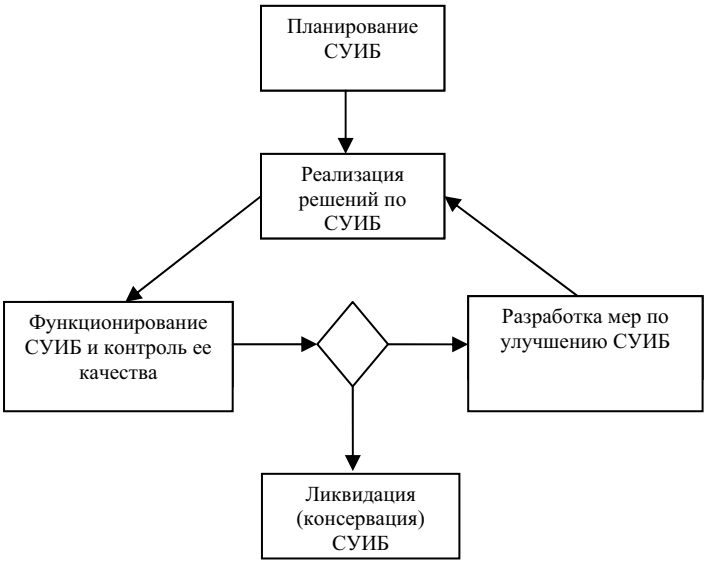

Рис. 2. Модель СУИБ на основе ПФУ

Видно, что данная модель не отражает в явном виде принципиального разделения труда по проектированию и реализации СУИБ на две составляющие – стратегическую и тактическую. Стратегическое прогнозирование делается один раз и заранее. Оно включает в себя 1-4 этапы ПФУ. Тактическая составляющая начинается с практической реализации

СУИБ (этап №5), включает ее адаптивную работу и совершенствование в процессе эксплуатации объекта (этап №6) и завершение работы (этап №7).

Исходя из этих соображений, оптимальную структурную схему СУИБ можно изобразить следующим образом (Рис. 2):

Данная модель в явном виде разделяет этапы проектирования и функционирования СУИБ и позволяет четко сформулировать требования по каждому этапу. Она же позволяет предъявить требования к квалификации персонала, занятого разработкой и обслуживанием СУИБ на каждом этапе.

1. *ISO/IEC 27001:2005* “Information technology – Security techniques – Information security management systems - Requirements”.
2. *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.

Поступила 6.10.2010р.

УДК 621.3

О.В. Чала, к.е.н., доцент (УкрДАЗТ)

ІНФОРМАЦІЙНИЙ ПРОСТІР ПІДПРИЄМСТВА ЯК ОБ’ЄКТ УПРАВЛІННЯ

В статті розглядається сутність правила і передумови побудови процесів для реалізації процесно-орієнтованого управління якістю на промисловому підприємстві. Запропоноване визначення процесу управління якістю, а також багаторівневу структуру процесу виробництва промислової продукції. Узагальнено та доповнено перелік правил щодо побудови процесів промислового підприємства для системи управління якістю.

В статье рассматривается сущность, правила и предпосылки построения процессов для реализации процесно-ориентированного управления качеством на промышленном предприятии. Предложено определение процесса управления качеством, а также многоуровневая структура процесса производства промышленной продукции. Обобщен и дополнен перечень правил построения процессов промышленного предприятия для системы управления качеством.

Essence is examined in the article, governed and pre-conditions of construction of processes for realization of processing-oriented management quality on an industrial enterprise. Determination of process of quality management, and multilevel structure of process of production of industrial goods, is offered. Generalized and complemented list of rules of construction of processes of industrial enterprise for control the system by quality.