УДК 004.413.4(043.2)

Волобуев Б.В., Черныш В.И.
Национальный университет радиоэлектроники, Харьков

ПРОБЛЕМАТИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Проект создания и внедрения корпоративной информационной системы (КИС) реализуется в условиях существенной неопределенности, которая проявляется в виде неполноты или неточности информации об условиях функционирования системы. Неопределенность сопутствует всем этапам жизненного цикла КИС. Модель жизненного цикла КИС включает ряд процессов: сбор информации; анализ; проектирование; реализация; внедрение; сопровождение.

Неопределенность, сопутствующая процессу проектирования КИС, может привести к созданию неблагоприятных ситуаций, которые будут препятствовать достижению поставленных целей в процессе проектирования КИС. Возможность проявления неблагоприятных ситуаций в проекте создания КИС характеризуется риском информационной безопасности (ИБ).

В докладе приводится необходимость организаций в цикле функционирования КИС процесса оценки и управления рисками ИБ. Процесс оценки рисками ИБ предполагает их идентификацию, количественную и/или качественную оценку и т.д.

Даются рекомендации по оценке рисков ИБ согласно международного стандарта ISO / IEC 27005: 2008. В данном стандарте процесс оценки рисков включает анализ и оценивание рисков ИБ.

Анализ возникающих рисков ИБ должен проводиться регулярно в процессе создания и эксплуатации КИС. Риски должны идентифицироваться, оцениваться и, на основе оценки, должны быть определены приоритеты рисков для КИС.

Оценка влияния риска ИБ для конкретной фазы жизненного цикла КИС может быть количественной и качественной. Количественные оценки базируются на имеющейся статистической информации и используемых моделях прогноза. При этом задача состоит в количественной оценке риска относительно других имеющихся рисков, и прогнозе влияния конкретного риска на проект информационной системы. Качественная оценка риска ИБ, как правило, базируется на экспертных оценках, которые могут быть получены, например, с использованием метода анализа иерархий.

Недостатком существующих подходов к анализу рисков ИБ является отсутствие единой методологической основы, позволяющей интегрировать как качественные, так и количественные подходы к оценке рисков.

Повышение эффективности оценки и управления рисками ИБ КИС может быть осуществлено путем формализации и автоматизации различных этапов анализа рисками. Решение данной задачи можно осуществить путем разработки методологии оценки рисков.

Научный руководитель – А.А.Замула, к.т.н., доц.