МОДЕЛЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

С.А. ТРУХАН

Под термином "управление информационными рисками" обычно понимается системный процесс идентификации, контроля и уменьшения информационных рисков компаний. Качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации.

Примерно с 1995 года в ряде высокотехнологичных стран мира проводятся ежегодные слушания по вопросам управления информационными рисками. Подготовлено более десятка различных стандартов и спецификаций, среди которых можно выделить следующие ISO 177992002 (BS 7799) [1], GAO и FISCAM, SCIP, NIST, AS/NZS 4360:2004 [2],[3], SAS 78/94 и COBIT. По этому трудно себе представить серьезную систему безопасности без модели управления рисками [4].

Рассмотрим основные принципы, которые закладываются в модель управления информационными рисками.

На первом этапе производится определение обстоятельств проведения оценки рисков. Это предполагает: краткий обзор целей предприятия; резюме целей всех заинтересованных лиц в оценке безопасности; выбор критериев, отражающих основные цели предприятия и позволяющие определить частоту или вероятность реализации риска и наносимый ущерб; выбор защищаемых активов; выбор ключевых элементов (тем), которые

будут рассматриваться последовательно в процессе определения рисков. Важно отметить, что эти темы должны включать в себя основные риски и не сильно затягивать этап определения рисков.

На втором этапе происходит определение рисков. Это предполагает выявление угроз и нежелательных инцидентов, которые могут привести к угрозам. Определение рисков изначально производиться с помощью методов контрольных списков, которые дополняются сессиями мозгового штурма с квалифицированными специалистами из разных областей. Данный подход позволяет максимально выявить и определить основные угрозы и нежелательные инциденты.

На третьем этапе производится анализ рисков. Этот этап предполагает: распределение рисков по родственным группам; определяется вероятность частоты появления рисков; определяется ущерб, наносимый риском; делаются предположения об уровне рисков. На данном этапе вводятся любые коэффициенты, которые будут отображать значение риска и участвовать в управлении риском. Для простых рисков могут находиться вероятности и строиться матрицы. Для сложных рисков, где вовлекается большое количество связанных событий, могут применяться некоторые методы моделирования. Независимо от детализации описания рисков, результат данного этапа – это начальное представление значений выявленных рисков, которые будут корректироваться на этапе оценки рисков.

На четвертом этапе производится оценка рисков, которая является критической для выявления наиболее важных рисков. В сложных ситуациях выявленные риски соотносятся с требованиями и целями предприятия. На основании данного анализа незначительные риски, в данном контексте, отбрасываются. Это позволяет сократить трудоемкость следующего этапа.

На пятом этапе рассматриваются методы "лечения" рисков. На этом этапе производится поиск методов уменьшения вероятности возникновения рисков или, если это невозможно, то поиск способов уменьшение наносимого ущерба. На данном этапе вводятся коэффициенты, которые отражают эффективность применяемых методов. На основании данных коэффициентов формируются планы стратегического поведения предприятия. Данные планы могут применяться для случаев возникновения выше выявленных рисков или вообще обходить данные риски на основании выбранной стратегии поведения предприятия.

Кроме пяти этапов в процессе управления рисками присутствуют ещё два процесса:

1. Процесс контроля и анализа, который присутствует на всех пяти этапах. Основной смысл данного процесса в следующем: в регулировании глубины изучения вопросов; в анализе внешних условий в ходе исследования и при их устаревании, в пересмотре результатов исследования с учетом современного состояния дел; в анализе затрат ресурсов на каждом этапе управления рисками, чтобы гарантировать рентабельность.

2. Процесс общения и консультирования, который присутствует на всех пяти этапах. Основной смысл данного процесса в следующем: в вовлечении максимального количества заинтересованных лиц в процесс оценки рисков; в выявлении наиболее актуальных рисков и определении степени последствий в исследуемой области; в том, что учтены все требования и цели со стороны предприятия.

В заключении хотелось бы заметить, что грамотное использование модели управления информационными рисками позволит получать очень хорошие результаты, наиболее важным из которых, является возможность экономического обоснования расходов предприятия на обеспечение информационной безопасности и непрерывности бизнеса. Экономически обоснованная стратегия управления рисками позволяет, в конечном итоге, экономить средства, избегая неоправданных расходов.

Литература

1. ISO/IEC 17799:2002 Information technology – Code of practice for information security management. International Organization for Standardization (2002);
2. Standards Australia and Standards New Zealand (2004) AS/NZS 4360:2004. Risk Management. Sydney. NSW. ISBN 0 7337 5904 1.
3. Standards Australia and Standards New Zealand (2004) HB 436:2004. Risk Management Guidelines: Companion to AS/XZS 4360:2004, Sydney, NSW. ISBN 0 7337 5960 2.
4. Сергей Петренко, Сергей Симонов, Методики и технологии управления информационными рисками, IT Manager, № 3/2003.