Общая структура изложения материала

написано Александр Астахов | 13 июня, 2023
Эта книга помимо предисловия, введения, библиографии, ссылок и приложений включает в себя семь глав.

Структура книги:

- *Глава 1. Предпосылки для управления информационными рисками*
- *Глава 2. Основные элементы управления информационными рисками*
- *Глава 3. Система управления информационными рисками*
- *Глава 4. Оценка рисков информационной безопасности*
- *Глава 5. Обработка рисков информационной безопасности*
- *Глава 6. Инструментальные средства для управления информационными рисками*
- *Глава 7. Практические рекомендации по внедрению системы управления информационными рисками*
- *Библиография*
- *Полезные ссылки*
- *Приложения*

Первая глава отвечает на вопрос первостепенной важности, без утвердительного ответа на который, возможно, и не стоило бы писать эту книгу: «Почему в наше время крайне важно управлять информационными рисками, а в недалеком будущем по причине недооценки информационных рисков человечество ожидают информационные кризисы, пострашнее нынешнего мирового финансового кризиса?» В первой главе книги мы попытаемся проложить дорогу между настоящим и будущим, показывая, почему

уже сейчас многие организации не могут обойтись без систематического управления рисками, почему сегодня нельзя относиться к управлению рисками, руководствуясь вчерашними представлениями, и почему завтра ситуация с информационными рисками может измениться кардинальным образом, что станет неожиданностью для многих людей, не успевших адаптироваться к стремительно изменяющимся обстоятельствам.

Во второй главе, опираясь на международные стандарты, мы дадим несколько равнозначных определений понятию «информационный риск», рассмотрим основные составляющие этого непростого понятия, факторы (элементы) риска, рассмотрим, чем обусловлено различие подходов к оценке рисков, применяемых в организациях. Мы также коснемся количественных и качественных способов определения величины риска, а заодно развеем распространенное заблуждение и покажем, что, несмотря на разнообразие способов вычисления рисков, не существует самодостаточных количественных или качественных подходов к оценке рисков, которые могли бы иметь прикладное значение, а в сущности, на практике имеет место комбинированный подход.

Как показывает опыт внедрения систем управления информационной безопасностью (СУИБ) в российских организациях и опыт их сертификации по требованиям международного стандарта ISO 27001, главной точкой преткновения обычно становится система управления рисками. В третьей главе мы рассмотрим эту систему, служащую базисом для СУИБ, в комплексе, опираясь на определяемую стандартами процессную модель. Если взглянуть на проблему широко, то мы увидим, что она не сводится лишь к двум ключевым процессам оценки и обработки риска. Для того чтобы система управления рисками оставалась жизнеспособной и могла адаптироваться к изменяющимся условиям, она должна включать в себя еще целый ряд процессов, обеспечивающих непрерывный контроль и совершенствование этой системы и теснейшим образом интегрированных со всеми остальными процессами СУИБ.

Четвертая глава является ключевой с точки зрения понимания используемой нами методологии оценки рисков. В ней шаг за

шагом рассматриваются все стадии этого процесса, начиная с инвентаризации активов и заканчивая формированием реестра информационных рисков. При этом мы не раскрываем каких-то секретов и в сущности не сообщаем каких-то сведений, которые сами по себе уже не были бы известны специалистам и не были бы описаны в стандартах. Мы склонны видеть свою заслугу, если мы вообще вправе на это претендовать, не в передаче некоего тайного знания, а скорее, в систематизации накопленного опыта и знаний профессионального сообщества, а также в переводе вопросов, которые обычно вызывают серьезные затруднения у многих специалистов, в практическую плоскость, разрешая их просто, сообразно сложившимся обстоятельствам и без излишнего теоретизирования.

Не так важно, какой подход к оценке рисков вы используете, а мы отнюдь не считаем, что наш подход является единственно возможным, главное – насколько адекватные и экономически оправданные решения по обработке рисков вы в конечном счете принимаете. В пятой главе книги мы рассмотрим возможные способы обработки рисков, механизмы планирования защитных мер и принятия решений по рискам, а также вопросы оценки возврата инвестиций в информационную безопасность. Основным результатом данных мероприятий служит разработка двух ключевых для СУИБ документов: Декларации о применимости механизмов контроля и Плана обработки рисков.

Шестая глава посвящена обзору наиболее популярных инструментальных средств управления рисками. Помимо этого мы рассмотрим проблему выбора специализированного программного инструментария для оценки рисков с различных точек зрения, а также плюсы и минусы, связанные с его использованием. Вопрос практической целесообразности применения подобного инструментария в конкретной ситуации мы оставим на усмотрение читателя.

В седьмой главе приводится ряд практических советов по внедрению системы управления информационными рисками, начиная с необходимых предпосылок для управления рисками, разработки

документации, формирования организационной структуры, проведения пилотного проекта и заканчивая полной оценкой рисков и поддержкой жизненного цикла процессов управления рисками.

В конце каждой главы приведен список несложных вопросов, над которыми рекомендуется самостоятельно поразмыслить, прежде чем переходить к чтению следующей. По ходу изложения материала предусмотрено также несколько практических заданий, которые мы выполняем на мастер-классе по управлению рисками, чтобы сохранить бодрость ума для лучшего восприятия материала и закрепить полученные знания. Читателю мы предлагаем не лениться и последовать нашему примеру, т.к., несмотря на все усилия автора, материал книги местами достаточно абстрактен и требует для своего восприятия свежего и подготовленного ума.

Информация справочного характера вынесена в Приложения.