Оценка рисков как основа корпоративного управления

написано Александр Астахов | 10 июня, 2023

Риск-ориентированный подход лежит в основе современного корпоративного управления. Оценка рисков позволяет принимать осознанные решения, правильно выбирая механизмы защиты и расставляя приоритеты. Базирующаяся на анализе рисков оценка возврата инвестиций от внедрения механизмов контроля позволяет менеджеру ИБ формировать бюджеты на безопасность и обосновывать планы по обеспечению безопасности с точки зрения экономической целесообразности, а не путем запугивания руководства организации чрезвычайными происшествиями или санкциями со стороны регулирующих органов. Оценка рисков позволяет избегать многих кризисных ситуаций. После кризиса остаются те, кто правильно управлял рисками (а также те, кому просто посчастливилось).

Оценка рисков позволяет:

- *из миллиона требований и средств защиты выбрать те, которые необходимы организации;*
- *принимать осознанные и своевременные решения относительно применения защитных мер;*
- *правильно расставлять приоритеты, формировать планы и бюджеты на безопасность;*
- *получить экономическое обоснование целесообразности применения защитных мер;*
- *оценить экономическую эффективность мер информационной безопасности;*
- *избежать кризисных ситуаций.*

Все современные стандарты и руководства в области корпоративного управления, включая стандарты на интегрированные системы управления (PAS 99), стандарты СУИБ (ISO 27001), банковские стандарты (СТО БР ИББС и Basel II), а также нормативные требования, предъявляемые к публичным компаниям (Turnbull и SoX), базируются на оценке рисков.

_____

Все современные стандарты корпоративного управления базируются на оценке рисков:

- *ISO 27001 (ГОСТ Р 27001);*
- *PAS 99;*
- *СТО БР ИББС;*
- *BaselII;*
- *UKCombined Code of Corporate Governance Turnbull Guidance (июль2003 г.);*
- *Sarbanes-Oxley Act of 2002 (SOX);*
- *COSO ERM-Integrated Framework.*

_____

COSO – организация, разрабатывающая стандарты внутреннего контроля для публичных компаний с целью обеспечения соответствия требованиям SoX и Turnbull, делает это на базе интегрированной структуры управления рисками предприятия. Систему управления информационными рисками (СУИР) следует рассматривать не как некую внутреннюю методику, используемую службой ИБ, как это часто бывает, а скорее, как часть интегрированной системы управления рисками (ERM).

В соответствии с Принципами Корпоративного Управления Организации Экономического Сотрудничества и Развития (OECD), хорошее корпоративное управление «…должно предоставлять надлежащие стимулы для правления и руководства к достижению

целей компании и ее владельцев и должно способствовать эффективному мониторингу», а эффективный мониторинг бизнес-процессов зависит от эффективности измерения рисков информационной безопасности. Эта директива непосредственно адресована крупным публичным компаниям, но очевидно, что оценка и управление информационными рисками входит в область интересов любого бизнеса.

В том время как корпоративное управление озабочено, главным образом, гарантиями прав акционеров и/или заинтересованных сторон в публичной компании, принципы корпоративного управления применимы к любой организации, особенно к тем, которые формируют часть цепочки поставок для публичной компании и в особенности, если какая-либо часть их бизнеса осуществляется в он-лайне. Способность организации гарантировать всем бизнес-партнерам, что принадлежащая им информация надежно защищена, является частью поддержки таких принципов управления, как открытость и прозрачность. Реализация этих принципов требует, в том числе, чтобы заинтересованным сторонам была доступна информация о существующих факторах риска.

Таким образом, эффективность организации, корпоративное управление, управление операционными рисками, а также законодательная и нормативная среда – все это служит побудительными причинами внедрения эффективной СУИР, которая так же важна для функционирования организации, как и эффективные информационные и телекоммуникационные системы.