Подходы к управлению рисками

написано Александр Астахов | 10 июня, 2023

Поскольку риски информационной безопасности являются основными далеко не для всех организаций, условно можно выделить три основных подхода к управлению этими рисками, различающиеся глубиной и уровнем формализма.

Различие подходов к управлению рисками:

- *Некритичные системы — применяется набор базовых требований безопасности, определяемых опытом, законодательством и стандартами.*
- *Критичные системы — высокоуровневая оценка рисков. Особое внимание на системы с наибольшим риском.*
- *Особо критичные системы — детальная оценка рисков с использованием формализованного подхода.*

Для некритичных систем, когда информационные активы являются вспомогательными, а уровень информатизации невысок, что характерно для большинства современных российских компаний, существует минимальная необходимость в оценке рисков. В таких организациях следует вести речь о некотором базовом уровне ИБ, определяемом существующими нормативами и стандартами, лучшими практиками, опытом, а также тем, как это делается в большинстве других организаций. Однако существующие стандарты, описывая некоторый базовый набор требований и механизмов безопасности, всегда оговаривают необходимость оценки рисков и экономической целесообразности применения тех или иных механизмов контроля для того, чтобы выбрать из общего набора требования и механизмов те их них, которые применимы в конкретной организации. Поэтому определенные элементы оценки информационных рисков требуются и для таких организаций.

Для критичных систем, в которых информационные активы не являются основными, однако уровень информатизации бизнес-процессов очень высок и информационные риски могут существенно повлиять на основные бизнес-процессы, оценку рисков применять необходимо, но в данном случае целесообразно ограничиться неформальными качественными подходами к решению этой задачи, уделяя особое внимание наиболее критичным системам.

Когда бизнес построен вокруг информационных активов и риски информационной безопасности являются основными, необходимо применять формальный подход и проводить детализированную оценку рисков по всем активам.

Во многих компаниях одновременно несколько видов активов могут являться жизненно важными, например, когда бизнес диверсифицирован или компания занимается созданием информационных продуктов и для нее могут быть одинаково важны и людские и информационные активы. В этом случае рациональный подход заключается в проведении высокоуровневой оценки рисков, с целью определения того, какие системы подвержены рискам в высокой степени и какие имеют критическое значение для ведения деловых операций, с последующим проведением детальной оценки рисков для выделенных систем. Для всех остальных некритичных систем целесообразно ограничиться применением базового подхода, принимая решения по управлению рисками на основании существующего опыта, экспертных заключений и лучшей практики.

Заметим, что со временем доля критичных и особо критичных информационных систем в организациях любой сферы деятельности неуклонном повышается.

Примеры организаций с высоким уровнем информационных рисков

Интернет-магазины, электронные биржи, расчетные системы, электронные торговые площадки	*Основной акцент – киберугрозы и действия инсайдеров.*
Производственные предприятия, использующие АСУТП	*Основной акцент: физические, техногенные и киберугрозы, защита коммерческой и государственной тайны.*
Телекоммуникационные компании	*Основной акцент – непрерывность предоставления услуг. Риски: техногенные, антропогенные, физические, киберугрозы.*
Банки, финансовые институты	*Основной акцент – защита финансовых транзакций, предотвращение утечки информации и действий инсайдеров.*

Международным стандартом ISO 27001 допускается использовать различные подходы к оценке рисков, однако далеко не любой подход будет удовлетворять требованиям этого стандарта.

В британском стандарте BS 7799-3 конкретизируются обязательные элементы, которые должен содержать процесс оценки рисков. Они включают в себя следующее:

- *Определение критериев принятия риска*. Эти критерии должны описывать обстоятельства, при которых организация намерена принимать риски.
- *Идентификация приемлемых уровней риска*. Какой бы подход к оценке рисков ни был выбран, должны быть идентифицированы уровни риска, которые организация считает приемлемыми.
- *Идентификация и оценка рисков*. Необходимо, чтобы выбранный подход к оценке рисков охватывал все факторы

риска, включая активы, угрозы, уязвимости, механизмы контроля и ущерб.

- *Охват всех аспектов области действия СУИБ*. Выбранный подход к оценке рисков должен охватывать все области контроля, содержащиеся в ISO 27001, Приложение А. Некоторые подходы к оценке рисков концентрируются только на ИТ, не учитывая физические, кадровые, организационные и законодательные аспекты. Такие подходы непригодны для оценки, требуемой в ISO 27001.
- *Учет каждого информационного актива (группы активов).* Риски должны оцениваться для каждого информационного актива, а не только для отдельных процессов или информационных систем.
- *Результаты оценки должны быть воспроизводимыми.* Выводы должны быть аргументированы таким образом, чтобы независимые эксперты, используя те же методы, могли бы получить аналогичные результаты.
- *Руководство организации должно принимать риски осознанно.* Другими словами, руководство должно осознавать реальные размеры и вероятность ущерба. Это достигается путем применения качественных и количественных шкал оценки риска и их калибровки в соответствии с правилами, описанными ниже.

Для того чтобы продемонстрировать свое соответствие стандарту ISO 27001, например, на сертификационном аудите СУИБ, организация должна не просто показать аудиторам таблицу с оценкой рисков, но также объяснить, на основании чего были получены такие оценки по всем элементам риска и по каждому информационному активу.

Обязательные элементы, которые должны быть отражены в выбранном организацией подходе к оценке рисков:

- *определение критериев принятия риска;*

- *идентификация приемлемых уровней риска;*
- *идентификация и оценка рисков;*
- *охват всех аспектов области действия СУИБ, всех активов и областей контроля;*
- *учет каждого информационного актива (группы активов);*
- *воспроизводимость результатов;*
- *осознанное принятие рисков руководством организации.*

Выбор подходов к оценке рисков определяется характером бизнеса организации и уровнем его информатизации, т.е. важностью для него информационных активов. Однако эффективность процесса управления рисками определяется не только точностью и полнотой анализа факторов риска и выбранным подходом, но также в значительной степени эффективностью механизмов принятия управленческих решений и контроля их исполнения, что целиком находится в компетенции высшего руководства организации.