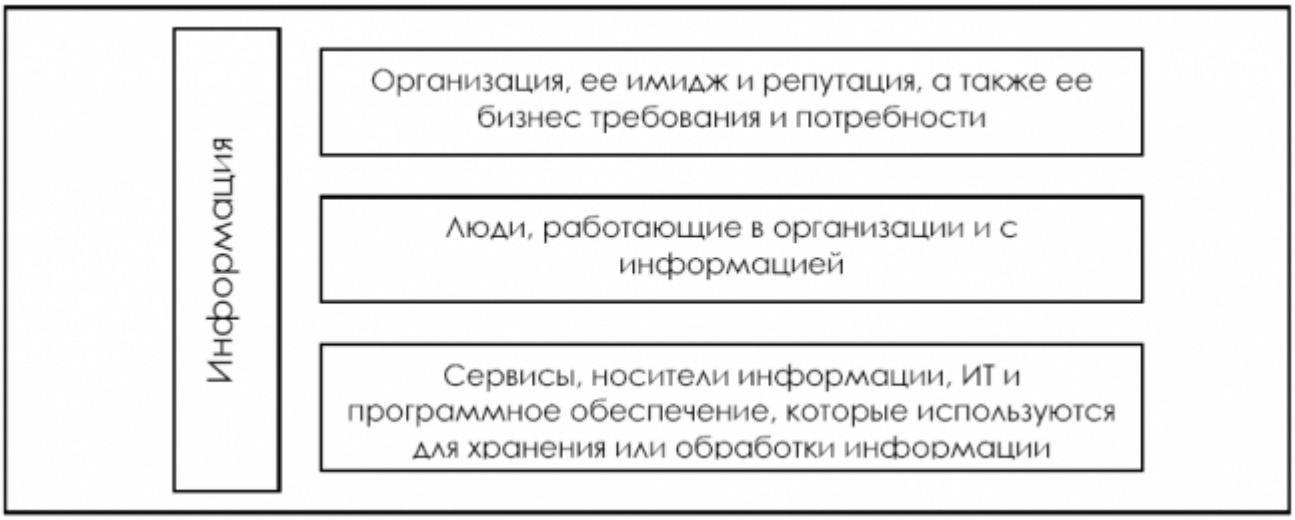
Активы организации как ключевые факторы риска

написано Александр Астахов | 10 июня, 2023

Ключевым элементом риска является актив, подверженный этому риску. Риски информационной безопасности обусловлены наличием у организации информационных активов. К информационным активам относится любая информация, представляющая ценность для организации. Они включают в себя информацию, напечатанную или записанную на бумаге, пересылаемую по почте или демонстрируемую в видеозаписях, передаваемую устно, информацию, хранимую в электронном виде на серверах, веб-сайтах, мобильных устройствах, магнитных и оптических носителях и т.п., информацию, обрабатываемую в корпоративных информационных системах и передаваемую по каналам связи, а также программное обеспечение: операционные системы, приложения, утилиты, программную документацию и т.п.



Помимо информации организация располагает и другими видами материальных и нематериальных активов, которые она использует для достижения своих бизнес-целей. Это имущество организации, имущественные и неимущественные права, интеллектуальная собственность, кадровые ресурсы, а также имидж и репутация организации. Современные международные стандарты также определяют еще одну категорию активов – это процессы, а также

информационные и неинформационные сервисы. Это агрегированные типы активов, которые оперируют другими активами для достижения бизнес-целей.

Виды активов организации

- *материальные;*
- *финансовые;*
- *имущественные и неимущественные права;*
- *интеллектуальная собственность;*
- *кадровые;*
- *информационные;*
- *процессы и сервисы;*
- *имидж и репутация.*

Все активы определенным образом взаимосвязаны. Реализация угроз в отношении одних активов, например помещений или оборудования, может приводить к нарушению безопасности других активов, например информации, хранимой в этих помещениях или обрабатываемой на данном оборудовании, и т.д. В свою очередь нарушение безопасности информации, например ее конфиденциальности или достоверности, может обуславливать финансовые или политические риски. Сбой сервера влияет на доступность хранящихся на нем информации и приложений, а его ремонт отвлекает людские ресурсы, создавая их дефицит на определенном участке работ и вызывая дезорганизацию бизнес-процессов, при этом временная недоступность клиентских сервисов может негативно повлиять на имидж компании.

Таким образом, во многих видах бизнес-рисков есть информационная составляющая, обусловленная тем, что все активы организации и соответствующие риски в отношении этих активов связаны между собой.

Рассмотрим, например, физические угрозы, такие как пожар или землетрясение. С этими угрозами связаны, прежде всего, риски для жизни и здоровья людей, также с ними связаны риски потери оборудования и помещений, нарушения бизнес-операций, а также риски потери информационных активов, которые размещаются на этом оборудовании и в этих помещениях. Мы видим, что с одной и той же угрозой связано множество активов и уязвимостей, т.е. множество различных рисков, которые находятся в сфере компетенции различных людей: работников службы безопасности, пожарников, кадровиков, IT-специалистов, специалистов по управлению непрерывностью бизнеса.

Поэтому руководству организации, вообще говоря, было бы проще рассматривать все эти взаимосвязанные бизнес-риски в совокупности, в рамках единого процесса и общей методологии, охватывающей все виды информационных, физических и операционных рисков.

Все виды активов важны для организации. Однако у каждой организации есть основные активы и есть вспомогательные. Определить, какой актив является основным и жизненно важным, очень просто, т.к. бизнес организации построен вокруг основного актива. Так, бизнес может быть построен на владении и использовании материальных активов (земля, недвижимость, оборудование, полезные ископаемые), бизнес может быть построен на управлении финансовыми активами (кредитные организации, страхование, инвестирование), бизнес может быть основан на компетенции и авторитете конкретных специалистов (консалтинг, аудит, обучение, высокотехнологичные и наукоемкие отрасли) или все может вращаться вокруг информационных активов (разработка ПО, информационных продуктов, электронная коммерция, бизнес в Интернет).

Риски основных активов чреваты потерей бизнеса и невосполнимыми потерями, поэтому на этих рисках в первую очередь сосредоточено внимание владельцев бизнеса и ими руководство организации занимается лично и в первую очередь. Риски вспомогательных активов приводят к восполнимому ущербу и

не являются основным приоритетом в системе управления организации. Обычно управлением такими рисками занимаются специально назначаемые люди, либо эти риски передаются, скажем, аутсорсинговой организации. Управление такими неосновными рисками – это вопрос эффективности управления, а не выживания для организации.